Învăţământul profesional şi tehnic în domeniul TIC

Proiect cofinanţat din Fondul Social European în cadrul POS DRU 2007-2013

Beneficiar – Centrul Naţional de Dezvoltare a Învăţământului Profesional şi Tehnic

str. Spiru Haret nr. 10-12, sector 1, Bucureşti-010176, tel. 021-3111162, fax. 021-3125498, vet@tvet.ro

COMUNICAŢII WIRELESS PENTRU ECHIPAMENTE DE CALCUL

Material de predare

Domeniul: Informatică

Calificarea: Tehnician echipamente de calcul

Nivel 3 avansat









2009

AUTOR:

CORNELIU-CONSTANTIN RUSU – profesor grad didactic I, Colegiul Tehnic „INFOEL” Bistriţa

COORDONATOR:

SIDOR COSTINAŞI - Prof. drd , Colegiul Tehnic „INFOEL” Bistriţa

CONSULTANŢĂ:

IOANA CÎRSTEA – expert CNDIPT

ZOICA VLĂDUŢ – expert CNDIPT

ANGELA POPESCU – expert CNDIPT

DANA STROIE – expert CNDIPT

Acest material a fost elaborat în cadrul proiectului *Învăţământul profesional şi tehnic în domeniul TIC,* proiect cofinanţat din Fondul Social European în cadrul POS DRU 2007-2013

Elemente grafice

Element	Semnificaţie
	Criterii de apreciere/ verificare
	Definiţie
	Listă de verficare; Paşi de urmat
	Atenţie! Informaţie importantă!
	Atenţie! Este interzis să...
	Recomandări cu privire la termene – limită; Alte recomandări cu privire la organizarea resurselor de timp.

Cuprins

I. Introducere

Materialele de predare reprezintă o resursă – suport pentru activitatea de predare, instrumente auxiliare care includ un mesaj sau o informaţie didactică.

Prezentul material de predare, se adresează cadrelor didactice care predau în cadrul şcolilor postliceale, domeniul **Informatică**, calificarea **Tehnician echipamente de calcul.**

El a fost elaborat pentru modulul **Comunicaţii wireless pentru echipamente de calcul**, ce se desfăşoară în 60 ore, în următoarea structură:

Pregătire teoretică 24 ore

Laborator tehnologic 32 ore

Instruire practică 4 ore

Competenţe	Teme	Fise suport
Descrie metode de comunicație wireless pentru echipamente de calcul	• Tema 1 **Metode de comunicație wireless pentru echipamentele de calcul**	• Fişa suport 1.1. Descrierea tehnologiei **bluetooth** • Fişa suport 1.2. Descrierea tehnologiei **infraroşu** • Fişa suport 1.3. Descrierea tehnologiei **WAN celulare** • Fişa suport 1.4. Descrierea tehnologiei **WI-FI** • Fişa suport 1.5. Descrierea tehnologiei **satelit**
	• Tema 2 **Realizarea unei reţele de comunicații folosind una din metodele de comunicație wireless**	• Fişa suport 2.1. Realizarea unei reţele wireless ad-hoc • Fişa suport 2.2 Realizarea unei reţele wireless cu acces point
Expune metode de	• Tema 3	• Fisa 3.1 Descrierea procesului de depanare

Competenţe	Teme	Fise suport
depanare pentru echipamente de calcul cu comunicaţii wireless	**Metodele de depanare pentru echipamente de calcul portabile**	a unui laptop
Expune metode de depanare pentru echipamente de calcul cu comunicaţii wireless	• Tema 4 **Depanarea unor echipamente de calcul portabile**	• Fisa 4.1 Înlocuirea acumulatorului şi hard disck-ului unui laptop • Fisa 4.2 Înlocuirea tastaturii unui laptop • Fisa 4.3 Înlocuirea modulelor de memorie ale unui laptop

Absolvenţii nivelului 3 avansat, şcoală postliceală, calificarea **Tehnician echipamente de calcul**, vor fi capabili să îndeplinească sarcini cu caracter tehnic de montaj, punere în funcţiune, întreţinere, exploatare şi reparare a echipamentelor de calcul.

II. Documente necesare pentru activitatea de predare

Pentru predarea conţinuturilor abordate în cadrul materialului de predare cadrul didactic are obligaţia de a studia următoarele documente:

- *Standardul de Pregătire Profesională* pentru calificarea Tehnician echipamente de calcul, nivelul 3 avansat – www.tvet.ro, secţiunea SPP sau www.edu.ro , secţiunea învăţământ preuniversitar
- *Curriculum* pentru calificarea Tehnician echipamente de calcul, nivelul 3 avansat – www.tvet.ro, secţiunea Curriculum sau www.edu.ro , secţiunea învăţământ preuniversitar

III. Resurse

Tema 1. Metode de comunicaţie wireless pentru echipamentele de calcul

Fişa suport 1.1. Descrierea tehnologiei bluetooth

Ce?



BLUETOOTH este o tehnologie de comunicaţii wireless „*fără fir*”, bazată pe undele radio, care permite schimbul de informaţii între două dispozitive.

Denumirea Bluetooth „dinte albastru” a fost adoptată în memoria unui rege danez din secolul X, Harald Bluetooth, care a unit Danemarca şi Norvegia cu scopul de a determina oamenii să comunice între ei. Astăzi tehnologia wireless Bluetooth permite oamenilor să comunice între ei, prin intermediul undelor radio şi cu un cost redus.



ÎNCEPUTUL

Ideea care a dat naştere tehnologiei wireless Bluetooth, a fost înlocuirea cablurilor de legătură dintre un telefon mobil şi un laptop, cu dispozitive radio de dimensiuni reduse încorporate în aceste echipamente, care să permită transmiterea de date şi voce între cele două echipamente. În anul 1994 un grup de ingineri de la compania de telefonie mobilă Ericsson încep investigarea fezabilităţii acestei tehnologii iar după un an apar primele rezultate.



EVOLUŢIA

Principalele probleme cu care s-au confruntat producătorii dispozitivele Bluetooth au fost: *interferenţa* cu alte dispozitive ce emit unde radio şi *interoperabilitatea defectuoasă* dintre două dispozitive fabricate de firme diferite. Pentru soluţionarea acestor probleme, în anul 1998 a luat fiinţă *Grupul de Interes Special* (SIG), care include companiile promotoare a tehnologiei wireless Bluetooth: *Ericsson, Motorola, Nokia, Toshiba, IBM, Intel, Microsoft* precum şi alte mii de companii asociate. Scopul acestui grup este

de a preveni devenirea acestei tehnologii proprietatea unei singure companii şi de a garanta interoperabilitatea globală între dispozitive indiferent de producător sau de ţara unde sunt utilizate. Grupul testează dispozitivele şi verifică dacă sunt îndeplinite cerinţele cu privire la: calitatea legăturii radio, informaţia specifică utilizatorului, profiluri şi protocoale. Din anul 1999 au apărut mai multe **versiuni Bluetooth**.

- **Bluetooth 1.0** Este prima versiune bluetooth care apare în anul 1999. Această versiune avea numeroase lipsuri şi probleme:
    - interferenţe cu alte aparate ce emit unde radio;
    - incompatibilitate în cazul în care echipamentele erau produse de firme diferite.

  Următoarea versiunea **1.1** lansată în februarie 2001, rezolvă o serie din aceste probleme.

- **Bluetooth 1.2** Versiune lansată în noiembrie 2003, este compatibilă cu versiunea **1.1** şi aduce îmbunătăţiri semnificative:
    - sunt mai rezistente la interferenţe cu alte aparate ce emit unde radio;
    - creşte calitatea semnalului audio;
    - creşte viteza transferului de date la 721 Kbps.

- **Bluetooth 2.0** Versiune lansată în noiembrie 2004, este compatibilă cu versiunile anterioare şi aduce următoarele îmbunătăţiri:
    - creşte viteza de transfer a datelor la 3,2 Mbps;
    - transport de semnale audio de calitate Wi-Fi si de semnale video;
    - alinierea Bluetooth la sistemele celulare 3G;
    - creşte raza de acţiune până la 100m;
    - consum de energie mai mic;
    - gestionare bună a conexiunilor între mai multe dispozitive;

- **Bluetooth 2.1** Versiune lansată în august 2007, este compatibilă cu versiunile anterioare şi aduce următoarele îmbunătăţiri:

- proceduri de securitate mai bune(inclusiv proceduri de criptare);
- o gestionare mai bună a consumului de energie;

- **Bluetooth 3.0** Versiune lansată în aprilie 2009, aduce următorele îmbunătăţiri:
  - viteza de transfer creşte până la 24 Mbps;
  - durată mai mare de viaţă pentru baterie;
  - sunt prevăzute cu dispozitiv Enhanced Power Control, care micşorează riscul deconectării accidentale.



PRODUSE BLUETOOTH

Primele produse în care a fost încorporată tehnologia wireless Bluetooth au apărut în perioada 2000-2001:

- Adaptoare pentru telefoane mobile, PC-uri şi laptop-uri (**fig.1.1.1 a**)
- Cartele pentru PC-uri şi laptop-uri (**fig.1.1.1 b**)
- Headset-ul Bluetooth (**fig.1.1.1 c**)
- PDA-uri (**fig.1.1.1 d**)
- PC-uri handheld (**fig.1.1.1 e**)
- Pocket PC (**fig.1.1.1 f**)









Figura 1.1.1 Produse Bluetooth

Din anul 2002 tehnologia Bluetooth este încorporată pe plăcile de bază ale PC-urilor şi laptop-urilor anumitor producători, în telefoanele mobile şi pe tot mai multe dispozitive mobile şi accesorii: imprimante, faxuri, camere foto digitale, tastaturi, mouse.

La ora actuală tehnologia Bluetooth este încorporată în produse industriale, medicale, dispozitive electronice pentru uz casnic, personale şi de afaceri, cu tendinţa de extindere în tot mai multe domenii. Odată cu extinderea producţiei de masă preţurile acestor produse vor scădea.



TEHNOLOGIA BLUETOOTH

Pe fondul creşterii accentuate a numărului de echipamente mobile de calcul şi a aplicaţiilor care presupun o mobilitate ridicată a utilizatorilor se remarcă din ce în ce mai mult o tendinţă de întrepătrundere a domeniului calculatoarelor cu cel al telecomunicaţiilor, liniile tradiţionale din acestea devenind tot mai puţin distincte. *Tehnologia wireless Bluetooth* este o tehnologie ideală pentru unificarea acestor "*două lumi*" permiţând tuturor tipurilor de dispozitive să comunice, ele transportând fie date, fie voce, fie pe amândouă.

În tehnologia Bluetooth, comunicaţia se face în ***radiofrecvenţă***, fiind folosită o bandă de frecvenţe nelicenţiată **ISM** (***Industrial Scientific and Medical***) între **2.402 GHz şi 2.480 GHz** alocată pentru domeniul industrial, ştiinţific, medical şi poate fi folosită astfel aproape oriunde în lume. Banda este divizată în **79 de canale radio**, fiecare canal având o

lărgime de bandă de **1 MHz**. Deoarece în această bandă mai operează şi alte tehnologii de comunicaţie, pentru eliminarea interferenţelor radio, Bluetooth foloseşte *tehnica de împrăştiere spectrală cu schimbare în salturi de frecvenţă*, această schimbare de frecvenţă producându-se de 1600 ori pe secundă. Fiecare dispozitiv având o gama de alegere a 79 de frecvenţe care se schimba de 1600 ori pe secundă, fiind puţin probabil ca două dispozitive să fie pe aceeaşi frecvenţa în acelaşi moment, iar dacă totuşi interferenţa are loc, ea durează doar o mică fracţiune de secundă.

O caracteristică de bază a tehnologiei Bluetooth este capabilitatea de a transmite şi recepţiona *simultan* atât *comunicaţiile vocale* cât şi *comunicaţiile de date*.

Comunicaţiile vocale
Bluetooth utilizează simultan 3 canale vocale sincrone sau un canal care suportă simultan transmisie vocală sincronă şi transmisie de date asincronă. Fiecare canal vocal suportă sincron 64 Kbps în fiecare sens.

Comunicaţiile de date
Un canal de date asincron poate suporta maxim 723,2 Kbps în sens direct în conexiune asimetrică sau 433,9 Kbps în conexiune simetrică.

Distanţa dintre două dispozitive între care se poate stabili un canal de comunicaţie depinde de clasa de putere. Tabelul 1.1.1 afişează cele trei clase de putere şi distanţa de conectare maximă specifică fiecăreia.

Tabelul 1.1.1

Clasa	**Puterea maximă admisă**		**Raza aproximativă de acţiune**
	[mW]	**[dBm]**	
Clasa 1	100 mW	20 dBm	100 metri
Clasa 2	2,5 mW	4 dBm	10 metri
Clasa 3	1mW	0 dBm	1 metru



ARHITECTURA BLUETOOTH

Tehnologia wireless Bluetooth permite dispozitivelor realizate de diverşi producători să lucreze împreună. Din acest considerent, arhitectura Bluetooth se defineşte atât ca un **sistem radio** cât şi ca o **stivă de protocoale** prin intermediul căreia este sesizată prezenţa altor dispozitive Bluetooth, sunt descoperite şi utilizate serviciile oferite de aceste dispozitive. Arhitectura Bluetooth este o îmbinare între o arhitectură hard şi o arhitectură soft.

ARHITECTURA HARD reprezintă partea fizică a dispozitivului Bluetooth (**fig.1.1.2**) şi este formată din:

- **Componenta analogică –** Bluetooth Radio
- **Componenta digitală –** Bluetooth Host Controller (**HC**)

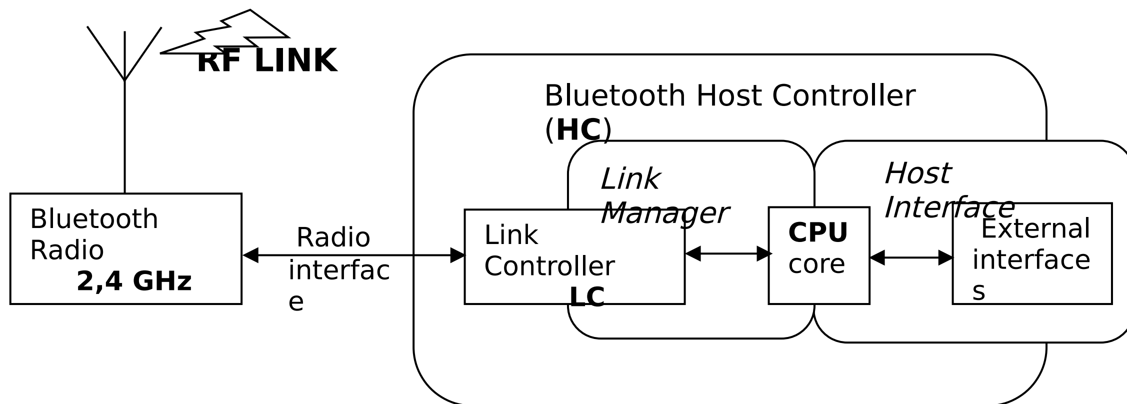


Figura 1.1.2 Arhitectura hard - Bluetooth

Bluetooth este un dispozitiv electronic analogic cu dublu rol de transmiţător ceptor (***transceiver***). Acest dispozitiv comunică pe de o parte cu niv adio din alt dispozitiv Bluetooth şi pe de altă parte cu link controller-ul ozitivului Bluetooth. Spre link contr există o dublă interfaţă logi ntru transportul datelor şi pentru tran l informaţiei de control între 2 părţi ale dispozitivului Bluetooth.

Host Contr este componenta digitală a dispozit Bluetooth care conţine:

- ***Link*** are mai multe funcţii: de lio, criptare. La nivelul Lin *ului Bluetooth* BD_ADDR (*etooth*.
- ***CPU core*** entra ivului Bluetooth care cuprinde st artea
- ***External i*** re modulul Bluetooth şi dispozitiv dulul Bluetooth.

ARHITECTURA S otocoale Bluetooth (**fig.1.1.3**)

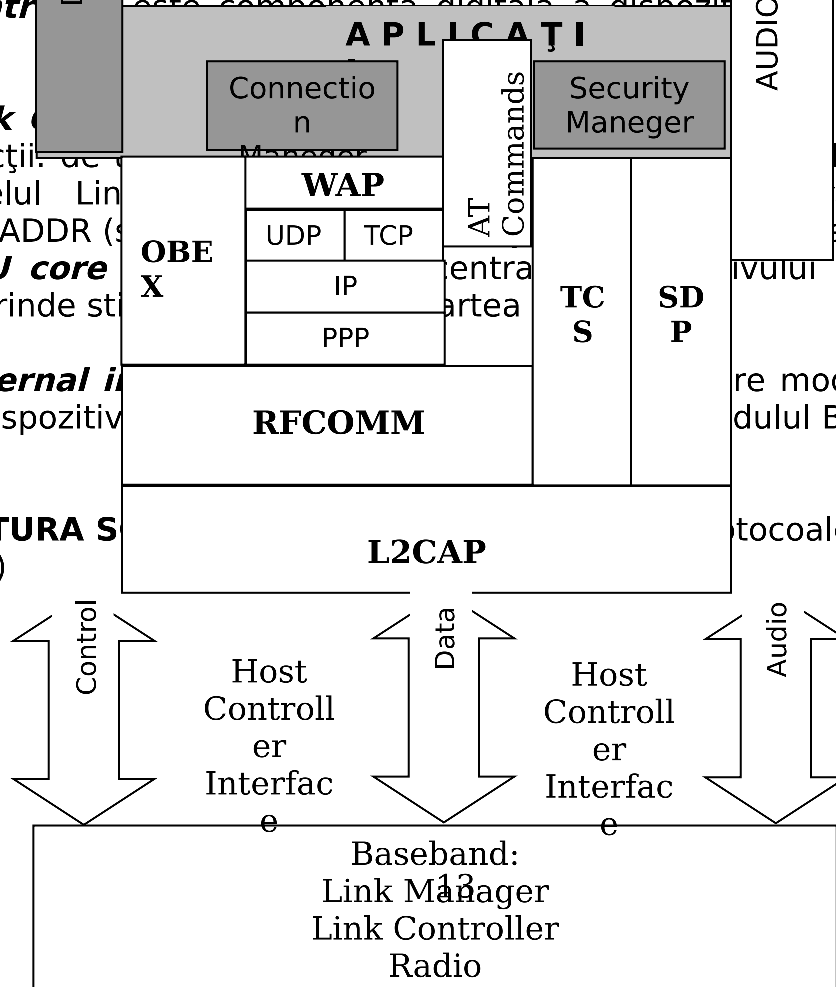


Figura 1.3 Stiva de protocoale Bluetooth

Potrivit acestor protocoale, dispozitivele Bluetooth se pot localiza, conecta şi schimba date între ele şi pot desfăşura aplicaţii interactive.

- **Baseband: Link Manager, Link Controller, Radio** – sunt ***protocoale de transport*** ce permit dispozitivelor Bluetooth să se localizeze între ele, permit crearea, configurarea şi administrarea legăturilor logice şi fizice pentru schimbul de date dintre protocoalele de niveluri superioare şi aplicaţii.
- **Host Controller Interface** – este o interfaţă comună între nucleul Blutooth şi gazda Bluetooth (ex. un laptop), care asigură compatibilitatea între diverse implementări hard.

- **L2CAP** (***Logical Link Control and Adaptation Protocol***) – protocol de control al legăturii logice şi adaptării prin care trece traficul de date. La nivelul L2CAP se face multiplexarea aplicaţiilor şi protocoalelor permiţând acestora să utilizeze în comun interfaţa aer. Tot aici se face segmentarea pachetelor de informaţie de dimensiuni mari adaptându-le la dimensiunea necesară transmisiunii la nivel baseband şi corespunzător reasamblarea pachetelor la recepţie.

- **RFCOMM** – este un port serial virtual pentru aplicaţii, care face posibilă desfăşurarea comunicaţiilor seriale peste legăturile wireless oferite de tehnologia Bluetooth.

- **WAP** (***Wireless Application Protocol***) – este un protocol pentru conectarea wireless la reţelele de internet şi este folosit de telefoanele mobile. Pentru conectarea la reţelele de internet prin dial-up se

utilizează protocolul **AT Commands**. Reţeaua accesată este o reţea de tip **TCP/IP** care foloseşte protocolul **IP**. După ce se stabileşte prin dial-up legătura cu reţeaua **TCP/IP**, dispozitivul care a iniţiat conexiunea foloseşte protocoalele standard din stiva Internet: **TCP**, **UDP**, **HTTP**, etc. Un dispozitiv se mai poate conecta la o reţea de tip **TCP/IP** printr-un punct de acces la reţea **PPP** (Point to Point Protocol) -aşa cum se procedează pentru accesul LAN. În acest caz, dispozitivul se conectează la punctul de acces la reţea printr-un link Bluetooth, iar la rândul său acesta se conectează la o reţea mai mare. Peste link-ul Bluetooth se foloseşte protocolul **PPP** din Internet. După ce s-a stabilit legătura prin acest protocol, pentru a interacţiona cu reţeaua sunt folosite protocoalele standard din stiva internet: **TCP**, **UDP**, **HTTP**. Accesul la o reţea **WAP** folosind un gateway de tip WAP se desfăşoară în mod similar cu diferenţa că în scopul interacţionării cu reţeaua se foloseşte protocolul **WAP**.

- **OBEX** (***Object Exchange***) – este un protocol de comunicare care permite schimbul de obiecte între două dispozitive Bluetooth, cum ar fi: cărţi de vizită electronice (formatul ***vCard***), ***e-mail-uri*** şi alte tipuri de mesaje (formatul ***vMessage***). OBEX este bazat pe modelul client-server şi oferă aceeaşi funcţionalitate ca şi **http** dar la un nivel mai redus.

- **TCS** (***Telephony Control Specification***) – este un protocol folosit pentru controlul comunicaţiilor telefonice cu flux audio sau de date. În cazul unui apel telefonic, după ce apelul este stabilit, semnalul vocal ce constituie convorbirea telefonică este transmis printr-un canal audio Bluetooth. În cazul conectării prin dial-up la o reţea, după ce apelul de date (data calls) este stabilit, conţinutul convorbirii este transmis sub formă de pachete de date prin intermediul protocolului L2CAP.

- **SDP** (***Service Discovery Protocol***) – este un protocol care stă la baza tuturor modelelor de utilizare, care defineşte o metodă standard prin care un dispozitiv Bluetooth descoperă şi află mai multe informaţii despre serviciile şi caracteristicile unui alt dispozitiv Bluetooth. Informaţiile descoperite pot fi tabelate în liste, cu ajutorul cărora utilizatorul, având informaţii despre serviciile dispozitivelor Bluetooth din vecinătate, poate selecta între aceste servicii şi stabilii conexiuni cu unul sau mai multe dispozitive Bluetooth.

- **Device Manager** – este un bloc care controlează comportamentul general al dispozitivului Bluetooth cum ar fi: administrarea numelui dispozitivului, cheile de link-uri memorate, detectarea altor dispozitive Bluetooth din vecinătate, conectarea la alte dispozitive Bluetooth

- **Grupul aplicaţiilor** – este constituit din aplicaţiile care efectiv utilizează legăturile Bluetooth. O parte din aceste aplicaţii sunt „moştenite” iar altă parte sunt proiectate pentru a folosi alte tehnologii care pot fi desfăşurate prin link-uri Bluetooth, cu modificări minore ale software-lui respectiv.



ARHITECTURA REŢELELOR BLUETOOTH

Unităţile Bluetooth aflate în acelaşi domeniu spaţial de acţiune radio pot realiza ***conexiuni punct-la-punct*** (**point-to-point**) şi/sau conexiuni ***punct-la-multipunct*** (**point-to-multipoint**), vezi **fig.1.1.4**. Unităţile pot fi adăugate sau deconectate în mod dinamic la reţea.

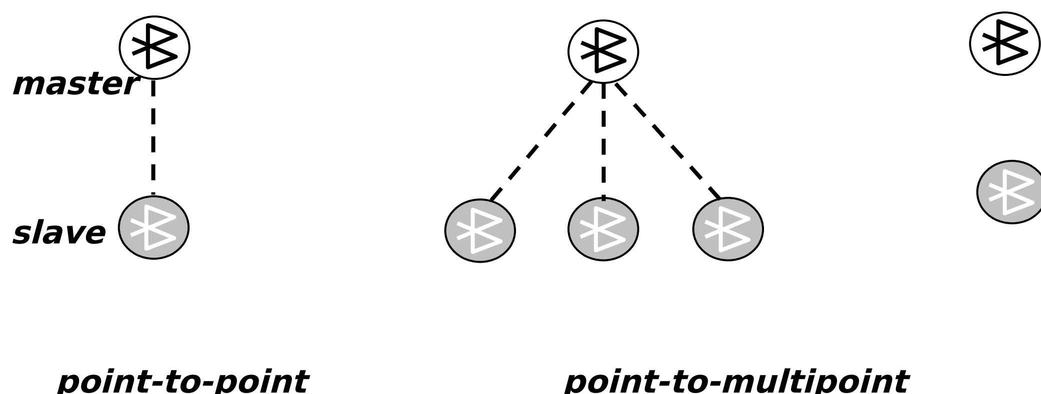


Figura 1.1.4 Moduri de conexiuni dintre unităţile Bluetooth

Când două dispozitive stabilesc o legătură Bluetooth, unul activează în rolul de ***master*** iar celălalt ca ***slave***, existând posibilitatea ca un dispozitiv oarecare să funcţioneze atât ca master într-o legătură cât şi ca slave într-o altă legătură.

Un ***master*** poate utiliza în comun un canal cu până la **7** dispozitive ***slave*** simultan active, sau încă 255 de dispozitive slave dacă acestea sunt în modul inactiv, reţeaua formată numindu-se ***piconet*** (***pico-reţea***), vezi **fig.1.1.5**.

Rolul de ***master*** nu conferă unui dispozitiv nici un fel de autoritate sau privilegiu, master-ul fiind responsabil de sincronizarea dispozitivelor legate la el. Toate dispozitivele **slave** care comunică cu un acelaşi master îşi schimbă frecvenţa în acelaşi timp cu master-ul.

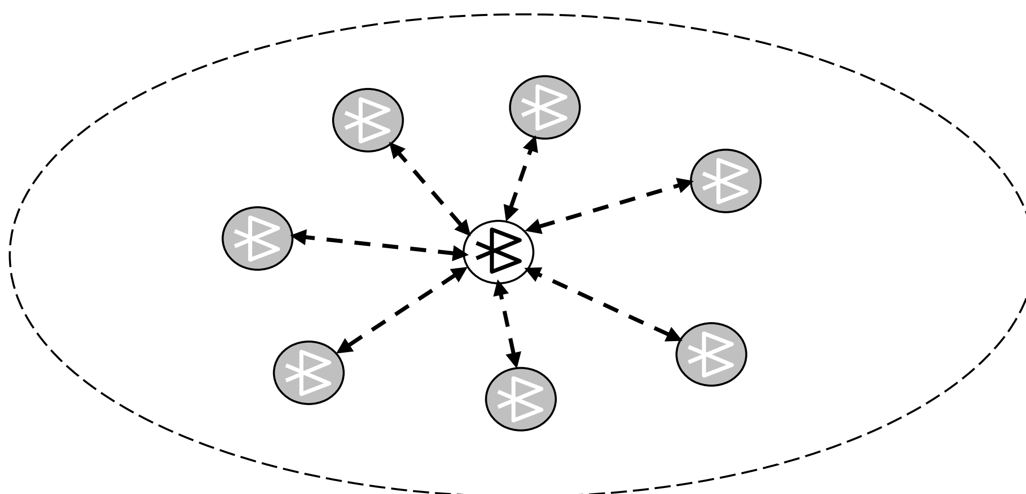


Figura 1.1.5 Piconet

Pentru a realiza configuraţii flexibile de comunicaţii şi schimburi de date, două sau mai multe ***piconets*** se pot intersecta şi formează un **scatternet**, fiind posibil ca unul dintre dispozitive să aibă rol de master într-un piconet şi de slave în alt piconet, vezi **fig.1.1.6**. Pentru a se respecta normele de imunitate la coliziuni între date, un ***scatternet*** poate cuprinde până la **10** ***piconet-uri***.

Dacă în acelaşi domeniu spaţial se află mai multe ***pico-reţele***, fiecare lucrează independent şi fiecare are acces la întreaga bandă de frecvenţă. Fiecare ***pico-reţea*** este stabilită pe un canal diferit, cu salt în frecvenţă. Toţi utilizatorii dintr-o ***pico-reţea*** sunt sincronizaţi pe canalul acesteia.

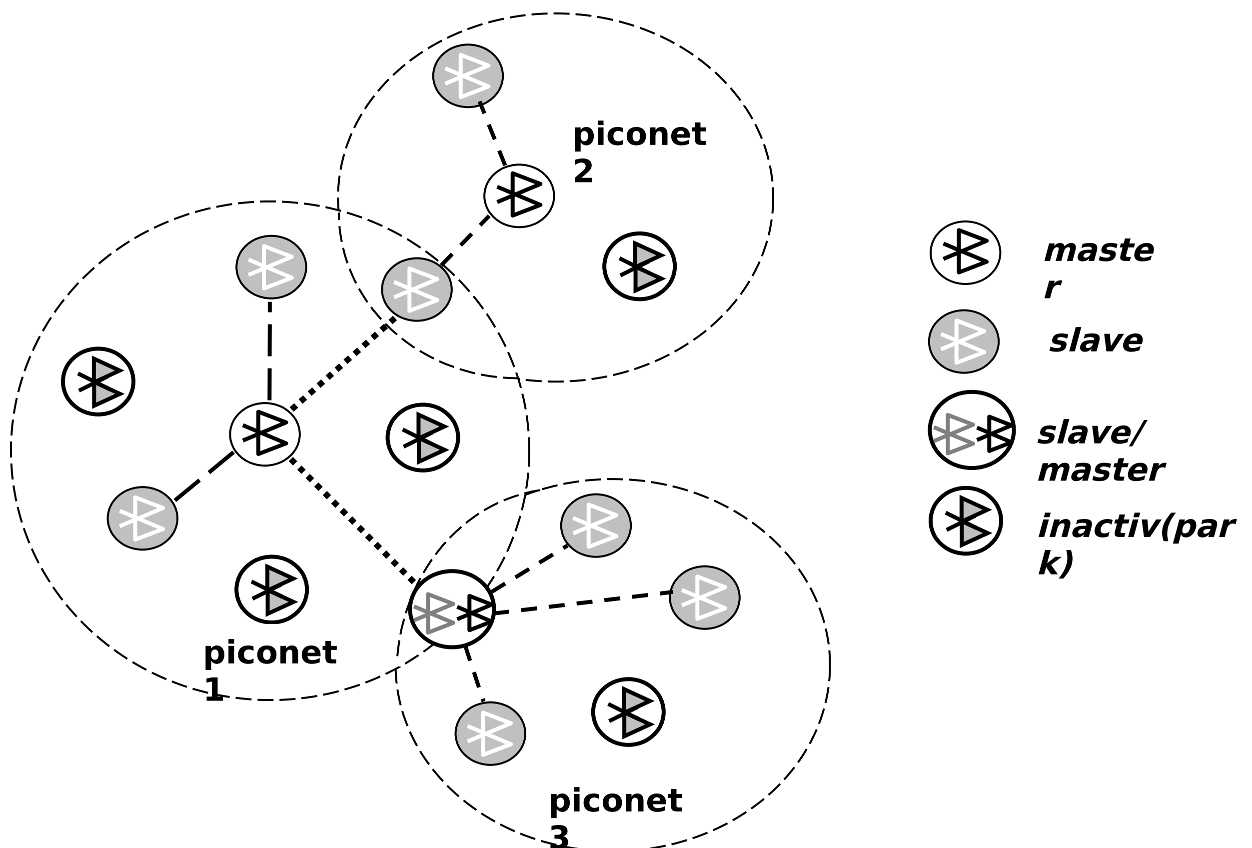


Figura 1.1.6 Scatternet

În prezent există foarte puţine implementări reale de scatternets datorită limitărilor de Bluetooth şi adresa de protocol MAC.



SECURITATEA REŢELEI BLUETOOTH

Deoarece semnalele radio pot fi uşor interceptate, dispozitivele Bluetooth au încorporate proceduri de securizare. Pentru simplitatea conectării a două dispozitive Bluetooth, majoritatea producătorilor acestor dispozitive aleg varianta configurării lor fără setări de securitate.

Standardul Bluetooth permite setarea a trei nivele de securitate:

Nivel 1 - No security(*mod nesigur)*. Dispozitivul permite conectarea oricărui alt dispozitiv. Dispozitivele configurate cu acest nivel nu implică nici un mecanism de securitate.

Nivel 2 - Service level security(*securitate la nivelul serviciului*). Măsurile de securitate sunt iniţiate după ce canalul de comunicaţie a fost stabilit. Suportă ***autentificare***, ***criptare*** şi ***autorizare***. Este cel mai flexibil nivel de securitate deorece pentru fiecare aplicaţie sau serviciu se poate aplica un anumit nivel de securitate. De exemplu pentru o bază de date importantă se poate aplica autentificare, criptare şi autorizare iar un anumit document să nu fie securizat.

Nivel 3 - Link level security(securitate la nivelul conexiunii*)*. Măsurile de securitate sunt iniţiate înainte de stabilirea comunicaţiei. Suportă ***autentificare*** şi ***criptare***. Autorizarea nu este necesară deoarece se presupune că două dispozitive conectate în nivelul 3, ar trebui să poată accesa toate aplicaţiile si serviciile disponibile pe fiecare dispozitiv. Acest nivel este cel mai securizat în schimb este mai puţin flexibil deoarece toată informaţia schimbată între două dispozitive este criptată.

Specificaţiile Bluetooth definesc un model de securitate bazat pe 3 componente:

- O rutină de interpelare pentru **autentificare**;
- Cifrarea fluxului informaţional ca metodă de **criptare**;
- Generarea unor chei de sesiune ca metodă de **autorizare**. Aceste chei pot fi oricând schimbate pe parcursul unei conexiuni stabilite.

În algoritmul de securizare sunt utilizate 3 entităţi:

- **Adresa dispozitivului Bluetooth (*BD_ADDR*)** (48 biţi), care este o entitate publică, unică pentru fiecare dispozitiv;
- **O cheie privată (*PIN*)** specifică utilizatorului (128 biţi), care este o entitate secretă care derivă din procedura de iniţializare;

- **Un număr aleator (*IN_RAND*)** (128 biţi), care diferă la fiecare nouă tranzacţie şi derivă dintr-un proces pseudo-aleator specific unităţii Bluetooth.



COMUNICAŢII BLUETOOTH

Tehnologia Bluetooth permite atât ***comunicaţii de date*** cât şi ***comunicaţii de voce*** şi ***audio***. Pentru efectuarea acestor comunicaţii, în specificaţiile Bluetooth există două tipuri de conexiuni fizice:

- **ACL(*Asynchronous ConnectionLess*)** – pentru **comunicaţii de date**. Aceste conexiuni lucrează până la 650 Kbps. Un dispozitiv cu rol de **master** poate avea un anumit număr de conexiuni ACL cu alte dispozitive, dar între două dispozitive poate exista doar o singură conexiune ACL. Conexiunile ACL asigură transmisii fără erori, ceea ce înseamnă că pachetele de date pierdute sau eronate sunt retransmise.
- **SCO(*Synchronous Connection Oriented*)** – pentru **comunicaţii vocale**. Aceste conexiuni lucrează la 64 Kbps şi pot stabilii 3 legături vocale simultane duplex sau se poate combina transmisia vocală cu una de date. Un dispozitiv cu rol de **master** poate avea 3 conexiuni SCO simultane, toate cu acelaşi dispozitiv **slave** sau cu 3 dispozitive **slave** diferite. Datorită ratei de transfer mici, conexiunile SCO nu sunt recomandate pentru transferuri audio de calitate sau transfeuri de date deoarece pachetele de date pierdute sau eronate nu sunt retransmise.

Deoarece între dispozitivele unei reţele wireless Bluetooth nu există cabluri de legătură, pentru realizarea comunicaţiilor între două dispozitive, aceste dispozitive trebuie în primul rând să se ***descopere şi să stabilească o legătură*** între ele, apoi să se ***conecteze la o bază de date*** şi în final să se **conecteze la un serviciu Bluetooth**.

- **Descoperirea dispozitivelor (*Inquiry*)** – este procedura prin care un dispozitiv Bluetooth **A** sondează vecinătatea cu un alt dispozitiv Bluetooth **B** din zonă şi cere adresa Bluetooth şi ceasul acestui dispozitiv în vedera sincronizării cu acesta. Pentru aceasta, dispozitivul Bluetooth **A** transmite o serie de pachete de interogare (**inquiry)** iar dispozitivul Bluetooth **B** răspunde cu un pachet **FHS(*Frequency Hop***

***Synchronisation*)** care conţine informaţiile necesare pentru crearea legăturii între cele două dispozitive (vezi **fig.1.1.7**). Dispozitivele Bluetooth se pot descoperii automat între ele dacă sunt setate pe modul **„inquiry scan”**, situaţie în care saltul de frecvenţă este mai lent iar timpul de descoperire este mai mare.

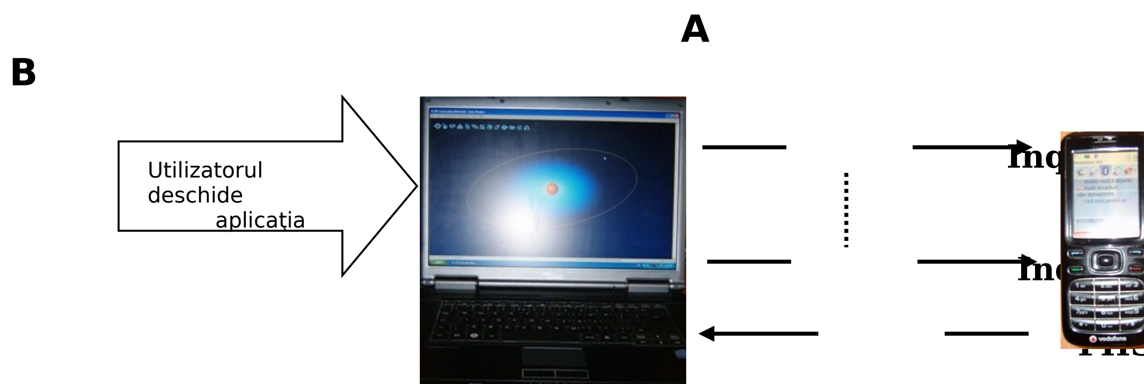


Figura 1.1.7 Schimb de mesaje între un laptop şi un telefon celular

Utilizatorul laptop-ului deschide o aplicaţie care necesită o legătură Bluetooth dial-up. Pentru a utiliza această aplicaţie laptop-ul trebuie să afle ce dispozitive Bluetooth sunt în zonă şi iniţializează o procedură **Inquiry**. Pentru aceasta, laptop-ul transmite o serie de pachete de interogare (***inquiry***) iar telefonul celular răspunde cu un pachet **FHS** care conţine toate informaţiile de care laptop-ul are nevoie pentru crearea unei legături cu celularul.

- **Stabilirea legăturii (*pairing*)** – este procedura prin care două dispozitive Bluetooth se autentifică între ele prin intermediul unei chei de autentificare. Dacă dispozitivele nu schimbă între ele o astfel de cheie, legătura nu poate fi realizată. Generarea unei chei de autentificare este cunoscută sub denumirea de ***pairing***. Procesul de **pairing** presupune generarea unei **chei de iniţializare**, a unei **chei de autentificare**, urmate de autentificare reciprocă (vezi **fig.1.1.8**).

  Cheia de iniţializare este bazată pe o cerere către utilizator, care este un număr personal de identificare (**PIN**) sau o parolă şi poate avea până la 128 biţi. Între 2 dispozitive parola este secretă. Cheia de iniţializare este folosită pentru criptare când se schimbă date pentru crearea cheii de autentificare, apoi este distrusă.

  Cheia de autentificare este bazată pe numere aleatoare şi pe adresele Bluetooth ale ambelor dispozitive.

Când procesul de ***pairing*** este complet, dispozitivele sunt autentificate reciproc. După stabilirea legăturii dispozitivele împart aceeaşi cheie de autentificare care este păstrată pentru utilizări viitoare.

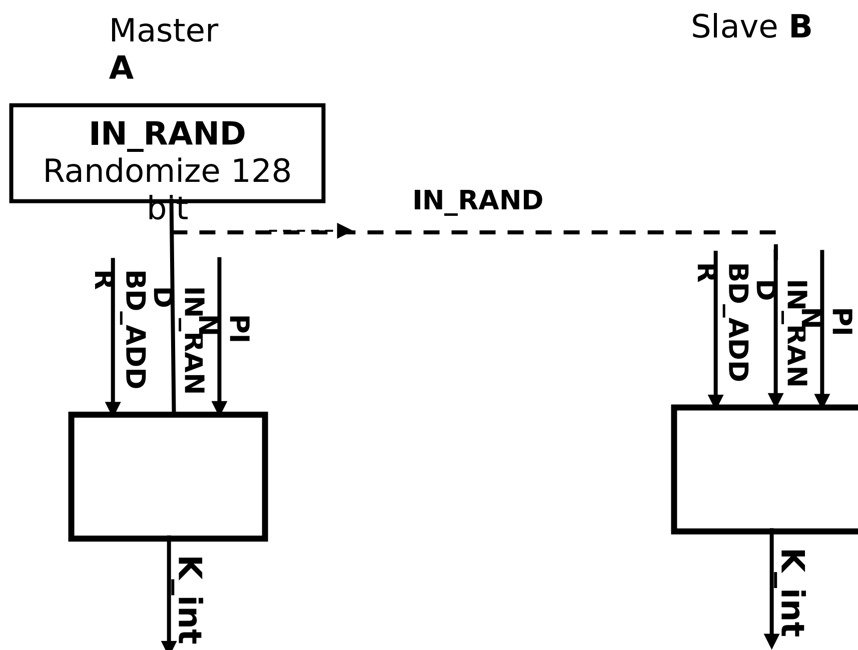


Figura 1.1.8 Crearea unei chei de iniţializare

➢ **Conectarea la o bază de date Service Discovery** – este necesară pentru a afla dacă un dispozitiv Bluetooth suportă un serviciu anume (**fig.1.1.9**).

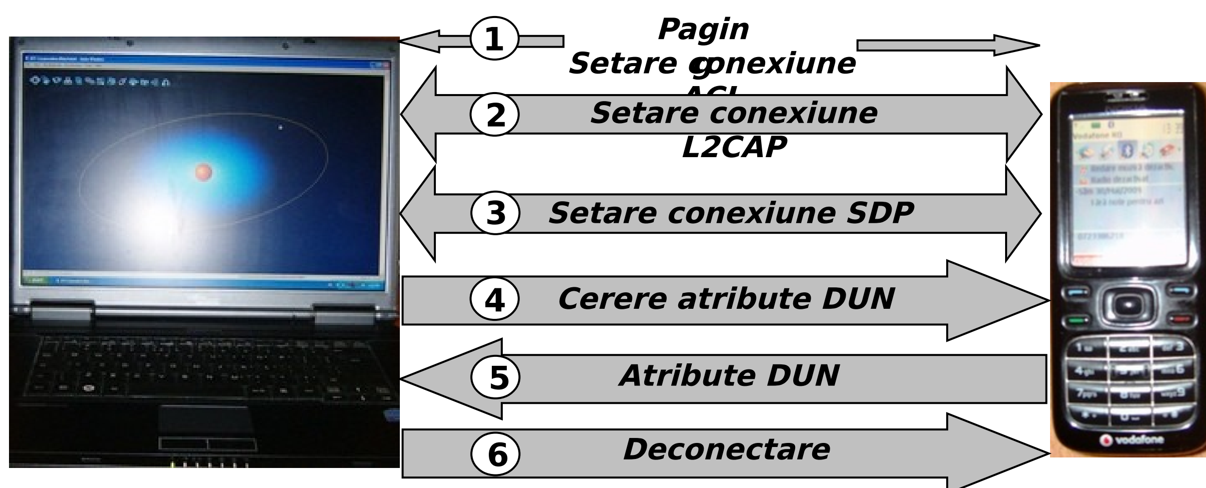


Figura 1.1.9 Secvenţe de conectare Laptop - Bluetooth la o bază de date



1. Laptop-ul trimite mesaje de ***paging*** telefonului celular, utilizând informaţiile adunate prin procedura ***inquiry***. Telefonul scanează mesajele de ***paging*** şi răspunde, moment în care, între cele două dispozitive se setează o conexiune **ACL** la nivelul benzii de bază pentru transferul de date.

2. După stabilirea conexiunii **ACL**, se realizează conexiunea la nivelul protocolului **L2CAP** utilizată de fiecare dată când are loc un transfer de date între dispozitive Bluetooth. Protocolul **L2CAP** permite mai multor servicii şi protocoale să utilizeze o singură legătură **ACL** în banda de bază.

3. Laptop-ul foloseşte canalul **L2CAP** pentru a seta o conexiune la serverul ***Service Discovery*** din telefonul celular.

4. Clientul ***Service Discovery*** din laptop solicită serverului ***Service Discovery*** din telefonul celular să-i trimită toate informaţiile pe care le posedă referitoare la profilul ***Dial-Up Networking (DUN)***.

5. Serverul ***Service Discovery*** din telefonul celular caută prin baza sa de date şi returnează caracteristicile referitoare la profilul ***Dial-Up Networking***.

6. După adunarea informaţiilor de descoperire a telefonului celular, se poate decide închiderea conexiunii cu acesta, dacă se doreşte stabilirea de conexiuni cu alte dispozitive din zonă în vederea colectării de informaţii prin ***Service Discovery***.

- **Conectarea la un serviciu Bluetooth** – este identic cu cel pentru conectarea în vedera descoperirii serviciilor (**fig.1.1.10**).

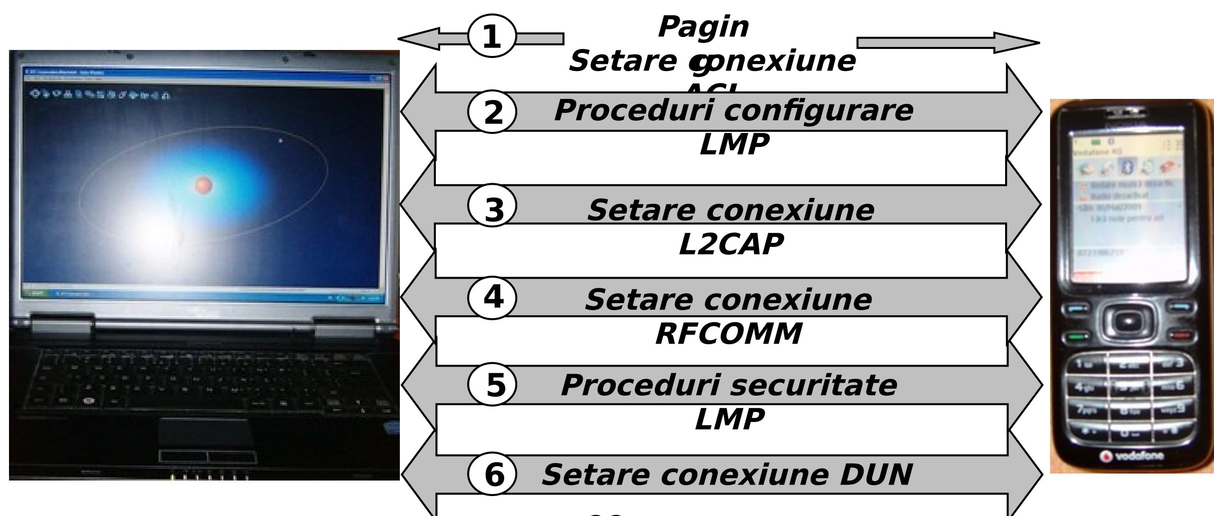


Figura 1.1.10 Secvenţe de conectare Laptop - Bluetooth la un serviciu Bluetooth



1. Aplicaţia care rulează pe laptop trimite mesaje de ***paging*** telefonului celular, utilizând informaţiile adunate prin procedura ***inquiry***. Telefonul scanează mesajele de ***paging*** şi răspunde, moment în care între cele două dispozitive se setează o conexiune **ACL** la nivelul benzii de bază pentru transferul de date. Aplicaţia de pe laptop trimite cerinţele sale către telefonul celular utilizând ***Host Controller Interface*** (**HCI**).

2. Managerul legăturii (**LM**), configurează legătura utilizând ***Link Manager Protocol*** (**LMP**).

3. După stabilirea conexiunii **ACL**, se realizează conexiunea la nivelul protocolului **L2CAP** utilizată de fiecare dată când are loc un transfer de date între dispozitive Bluetooth.

4. După stabilirea legăturii **L2CAP**, prin intermediul ei este setată o legătură **RFCOMM** (un simulator al interfeţei RS-232). **RFCOMM** multiplexeză câteva servicii şi protocoale într-o singură conexiune.

5. Fiecărui serviciu sau protocol i se atribuie un număr propriu de canal. Laptop-ul, în urma procedurii ***Service Discovery***, ştie ce număr de canal (***Dial-Up Networking*)** să folosească de la telefonul mobil.

6. Prin intermediul legăturii **RFCOMM** se setează conexiunea ***Dial-Up Networking*** (**DUN**) şi laptop-ul poate să înceapă exploatarea serviciilor **DUN** oferite de telefonul celular.



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- sala de clasă
- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea.
- Se poate aplica o lecţie de laborator cu tema: **"Instalarea unui dispozitiv Bluetooth"**

- Clasa poate fi organizată frontal sau pe grupe

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic

- Fişe de lucru pentru elevi

- Fişă de laborator

- Dispozitive Bluetooth



Ca probe de evaluare se pot folosi:

- Probe orale
- Teste scrise

Fişa suport 1.2. Descrierea tehnologiei infraroşu

Ce?



RADIAŢIILE INFRAROŞU) sunt radiaţii electromagnetice invizibile cu lungi de undă mai lungă decât cea a luminii vizibile dar mai scurtă decât a undelor radio. Cuvântul ***infra*** provine din latină şi înseamnă „***sub***", prin infraroşu este caracterizat domeniul situat „sub capătul roşu" al spectrului de lumină vizibilă (**fig.1.2.1**).

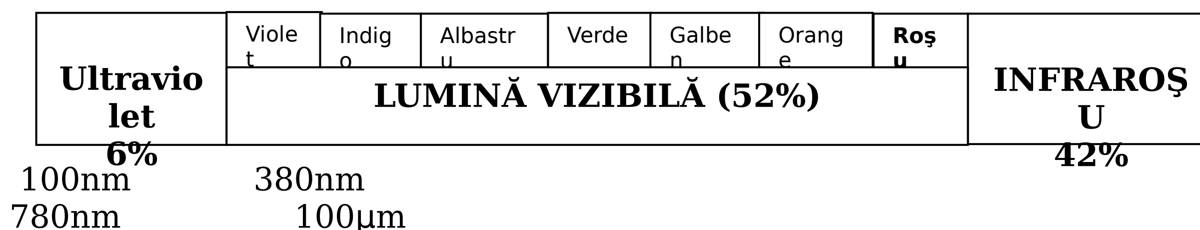


Figura 1.2.1 Spectrul radiaţiilor luminoase



SCHEMA BLOC A UNUI SISTEM DE COMUNICAŢIE ÎN INFRAROŞU

Schema bloc funcţională a unui sistem de comunicaţie în infraroşu este prezentată în **figura 1.2.2**:

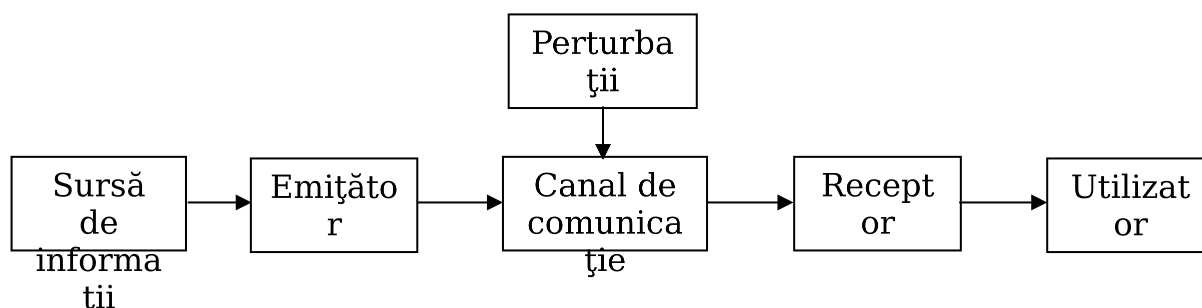


Figura 1.2.2 Schema bloc a unui sistem de comunicaţie în infraroşu

- **Sursa de informaţii** – pachete de date sub formă de semnale electrice logice.

- **Emiţătorul** – are rolul de a prelucra semnalul de intrare prin filtrare, amplificare, modulare, şi de a transmite acest semnal către un receptor. Emiţătorul este o diodă emiţătoare de lumină - LED (Light Emitting Diodes) care transformă un semnal electric în radiaţie luminoasă.

- **Canalul de comunicaţie** – este constituit din spectrul infraroşu al radiaţiilor electromagnetice.

- **Receptorul** – are rolul de extrage cât mai fidel, prin demodulare, informaţiile din semnalul transmis. Receptorul este o fotodiodă care transformă radiaţia luminoasă în semnal electric.

- **Utilizatorul** – preia pachetele de date furnizate de receptor



TIPURI DE CONEXIUNI ÎN INFRAROŞU

Clasificarea conexiunilor în IR se face după următoarele criterii:

1. **Din punct de vedere al gradului de direcţionare dintre emiţător şi receptor:**

   - **Directe** – când emiţătorul şi receptorul sunt situate pe aceaşi direcţie;

   - **Indirecte** – când emiţătorul şi receptorul nu sunt aliniate, dar au un unghi mare de cuprindere;

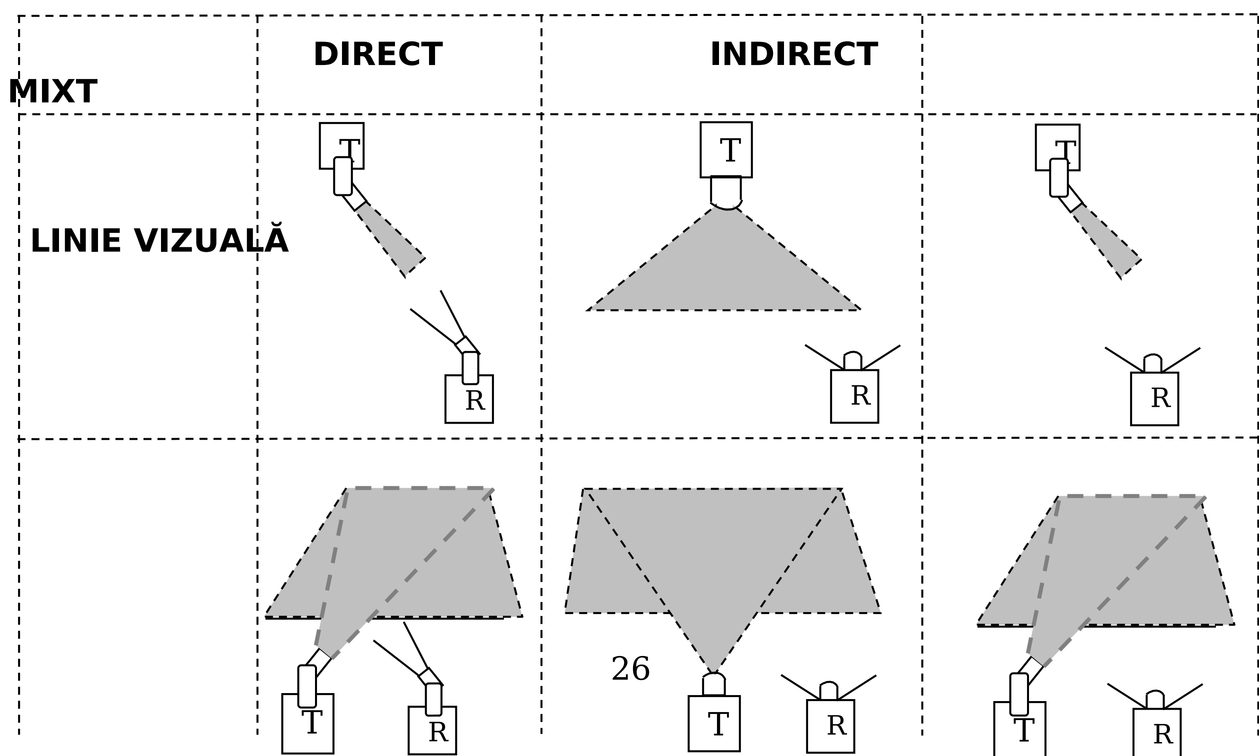
   - **Mixte** – sunt combinate cele două metode de mai sus.

2. **Din punct de vedere al căii de vizibilitate optică dintre emiţător şi receptor:**

   - **Line of sight** (***Linie vizuală***) – semnalul este transmis doar dacă între emiţător şi receptor este o vedere clară, neblocată;

   - **Scatter** (***Împrăştiată***) – semnalul este deviat de tavan şi de pereţi prin reflecţia luminii infraroşii;

   - **Reflective** (***Reflexivă***) – semnalul este transmis unui transceiver(emiţător-receptor) optic şi este redirecţionat către un receptor;



ÎMPRĂŞTIATĂ

Figura 1.2.3 Tipuri de conexiuni în infraroşu



INFRARED DATA ASSOCIATION (**IrDA**)

Pentru a standardiza comunicaţiile în infraroşu, în anul 1993 este creată asociaţia ***Infrared Data Association*** (**IrDA**). IrDA defineşte un set de standarde care specifica felul în care se transmit datele fără fir, prin intermediul radiaţiei infraroşii. Specificaţiile IrDA se referă atât la dispozitivele hardware implicate în comunicaţiile de date cât şi la protocoalele folosite.



STIVA DE PROTOCOALE IrDA

O stivă de protocoale IrDA, este un set de protocoale, organizat pe mai multe nivele, fiecare având un set de sarcini (**fig.1.2.4**).

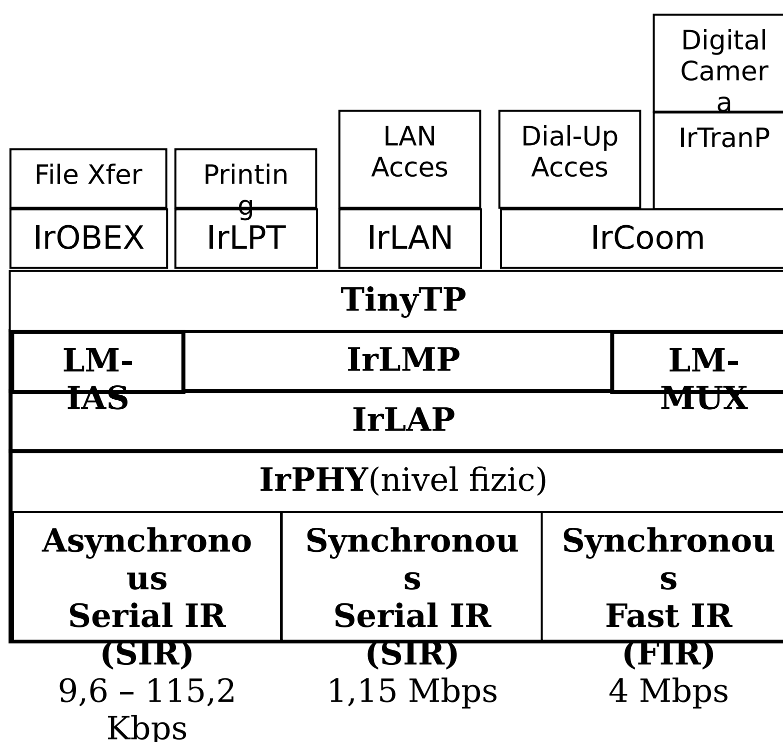


Figura 1.2.4 Stiva de protocoale IrDA

Nivelele obligatorii sunt:

- **IrPHY (*Infrared Physical Layer*)** – specifică codificarea şi formatul datelor.
  - Se bazează pe protocolul **HDLC** (***High-level Data Link Control***)
  - Raza de acţiune standard: 1 m
  - Unghiul de deflexie: ±15º
  - Viteza de transmisie: între 2,4 Kbps şi 16 Mbps

- **IrLAP** (***Infrared Link Access Protocol***) – reprezintă nivelul legăturilor de date.
  - Se bazează pe protocolul **HDLC**.
  - Descoperă dispozitivele din zonă cu care poate comunica
  - Stabileşte o conexiune bidirecţională
  - Stabileşte comunicaţia între un dispozitiv primar şi un dispozitiv secundar
  - Asigură transferul efectiv de date

- **IrLMP** (***Infrared Link Management Protocol***) – gestionează serviciile de conectare. Acest protocol este format din două părţi:
  - **LM - IAS** (***Link Management Information Access Service***) – protocol de interogare pentru determinarea serviciilor disponibile
  - **LM – MUX** (***Link Management Multiplexer***) - oferă multiple canale logice

Nivelele opţionale sunt:

- **Tiny TP (*Tiny Transport Protocol*)** – oferă:
  - Transportul mesajelor prin segmentare
  - Controlul fluxului de date

- **IrOBEX (*Infrared Object Exchange Protocol*)** – gestionează transferul de obiecte, fişiere sau alte blocuri de date.

- **IrCOMM (*Infrared Communication Protocol*)** – este emulator de porturi seriale şi paralele, permiţând aplicaţiilor existente(bazate pe comunicaţii paralele şi seriale) să folosească comunicaţia IR fără modificări.

- **IrLAN (*Infrared Local Area Network*)** – oferă posibilitatea conectării unui dispozitiv IR la o reţea locală. Sunt 3 metode de conectare:

    - **Peer to peer** – punct la punct
    - **Acces Point** – punct de acces
    - **Hosted** – gazdă

- **IrLPT (*Infrared Line Printer*)** – este un protocol de utilizare a unei imprimante prevăzute cu dispozitiv IR.



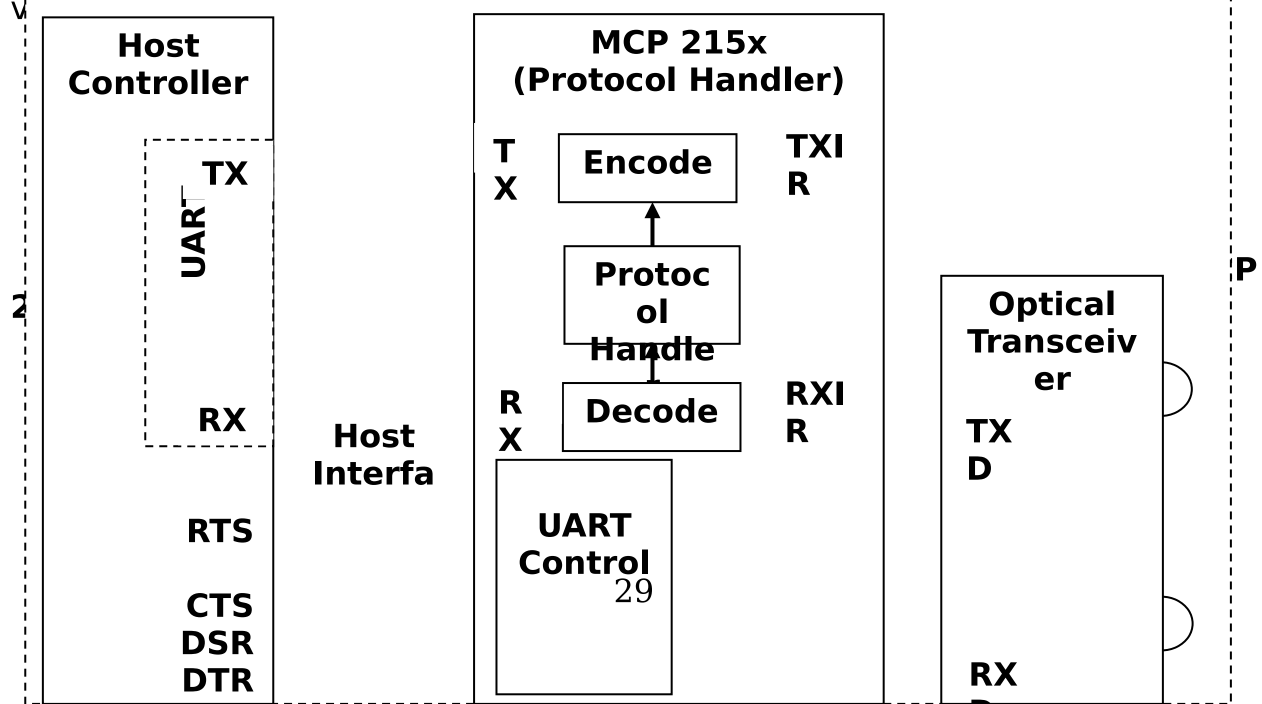
ECHIPAMENTE IrDA

Conform standardului **IrLAP** (***Infrared Link Access Protocol***) echimapentele IrDA se clasifică în două categorii:

- **Staţii primare** – care solicită şi controlează realizarea unei legăturii
- **Staţii secundare** – care răspunde la solicitările staţiei primare

Într-o conexiune IrDA poate exista numai o singură staţie primară şi mai multe staţii secundare. O staţie primară poate adresa o singură staţie secundară dar poate transmite date tuturor staţiilor secundare din zonă. O staţie secundară poate transmite date doar unei staţii primare.

Există multe firme care produc circuite pentru transferul de date IrDA. Ca v



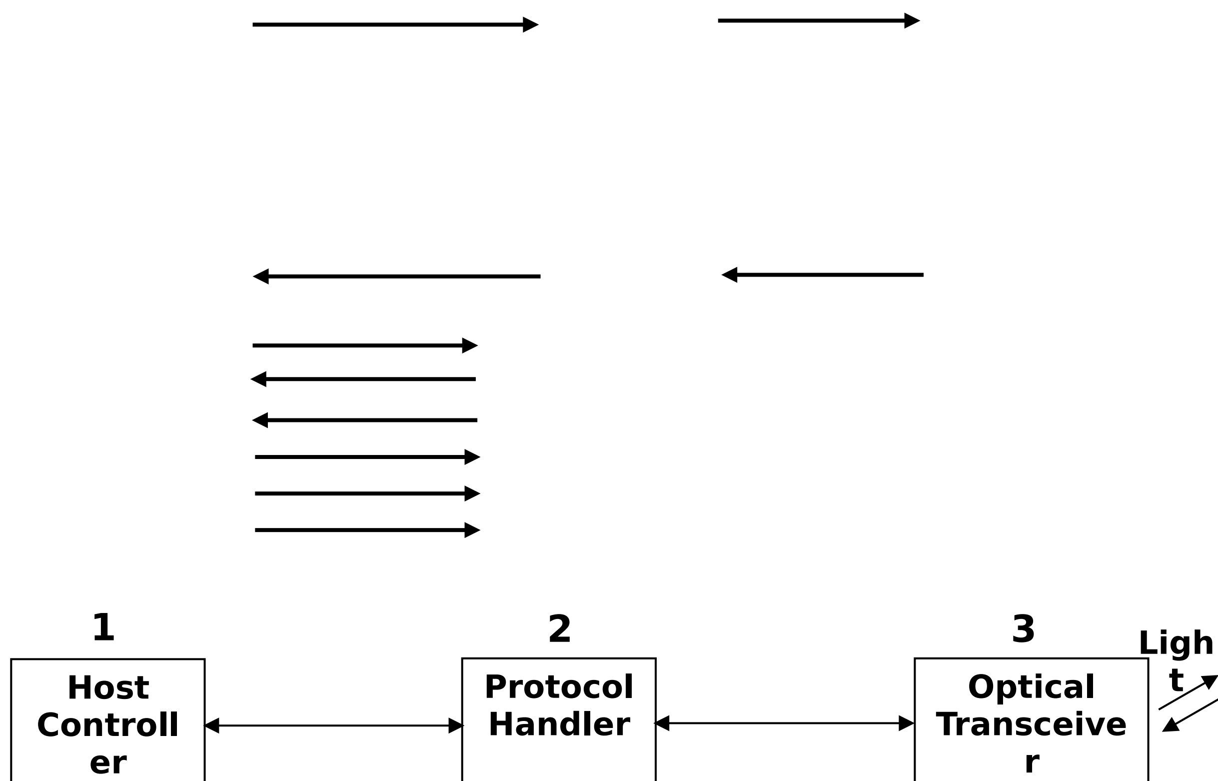


Figura 1.2.5 Schema bloc a interfeţei IrDA cu microcontroller MCP 215x

UART (***Universal Asynchronous Receiver/Transmiter***) – este un circuit integrat care coordonează întreaga comunicaţie serială şi conţine softul de programare necesar controlului portului serial. Acest circuit transmite şi recepţionează date printr-un port serial. Circuitul UART conţine mai mulţi regiştrii cu rol important în realizarea comunicaţiei.

Comunicaţia serială este definită de standardul **RS 232**. O legătură de bază RS 232 necesită trei conexiuni:

- conexiune pentru **transmisia datelor**
- conexiune pentru **recepţia datelor**
- conexiune pentru **controlul fluxului de date**

Semnalele interfeţei seriale conform standardului RS 232 sunt:

- **Transmit Data – TD** (***Transmisie date***) – pe această linie, datele sunt transmise serial de către calculator. Pentru transmisie este necesar ca semnalele: **RTS**, **CTS**, **DTR**, **DSR** să fie active.
- **Receive Data – RD** (***Recepţie date***) – pe această linie, datele sunt recepţionate de la un echipament extern.
- **Data Terminal Ready – DTR** (***Terminal de date operaţional***) – semnalul DTR este activat când calculatorul este pregătit pentru comunicaţia de date.

- **Data Set Ready – DSR** (***Echipament extern operaţional***) – semnalul DSR este activat când echipamentul extern este pregătit pentru comunicaţia de date.

- **Request to Send – RTS** (***Cerere de emisie***) – semnalul RTS este activat când calculatorul este pregătit pentru transmisia datelor.

- **Clear to Send –CTS** (***Gata de emisie***) – semnalul CTS este activat când echipamentul extern este pregătit pentru recepţia datelor de la calculator.

- **Carrier Detect – CT** (***Detectare purtătoare de semnal***) – semnalul CT este activat când echipamentul extern detectează semnalul purtător al altui echipament extern din zonă.

- **Ring Indicator – RI** (***Indicator de apel***) – semnalul Ri este activat când echipamentul extern detectează semnal de apel de la alt echipament extern.

- **Transmit Clock – TC** (***Ceas pentru transmisie***) – este semnalul de ceas pentru transmisie furnizat calculatorului de către echipamentul extern în cazul unei comunicaţii sincrone.

- **Receive Clock – RC** (***Ceas pentru recepţie***) - este semnalul de ceas pentru recepţie furnizat calculatorului de către echipamentul extern în cazul unei comunicaţii sincrone.



TRANSMITEREA DATELOR ÎN IR

Transferul de date în infraroşu a fost destinat să înlocuiască transferul serial **RS 232**, în mod **half – duplex**. Datele sunt comunicate în mod half-duplex, deoarece în timp ce transmite, receptorul dispozitivului este „orbit” de lumina propriului transmiţător şi de aceea comunicarea full-duplex nu este optimă.

Rata de transmisie se împarte în 4 categorii:

- ***Serial Infrared*** (**SIR**) – distanţa de comunicare este de maxim 1 m la lumina zilei, sub un unghi de deflexie de 15º. Viteza de transmisie acoperă vitezele de transmisie suportate de portul RS 232 (9600 bps; 19,2 Kbps; 38,4 Kbps; 57,6 Kbps; 115,2 Kbps).
- ***Medium Infrared*** (**MIR**) – viteze de transmisie: 57,6 Kbps şi 115,2 Kbps.

- ***Fast Infrared*** (**FIR**) – viteză de transmisie până la 4 Mbps

- ***Very Fast Infrared*** (**VFI**) – viteză de transmisie până la 16 Mbps

Pentru viteze mari de transfer, datele sunt transferate sub formă de pachete sau cadre. Un cadru poate avea între 5 şi 2050 octeţi (vezi **Tabelul 1.2.1**)

DENUMIRE	DEFINIŢIE	LUNGIME
STA	Octet de start	**8 biţi C0h**
ADDR	Câmp de adresă	**8 biţi**
DATA	Câmp de control date	**8 biţi**
DATA	Câmp de date	**245 octeţi**
FCS	Câmp detectare şi corectare erori	**16 biţi**
STO	Octet de stop	**8 biţi C1h**

Tabel 1.2.1 Structura cadrului

Câmpul de date trebuie sa fie multiplu de 8 biţi. Câmpul de date este opţional, deoarece unele cadre (cadrele de comandă) nu conţin date.

Formatul unui cadru este definit în standardul **IrLAP** (***Infrared Link Access Protocol***). Acest protocol este bazat pe transmisia serială **RS 232**, în mod sincron sau asincron, cu protocolul **HDLC** (***High-level Data Link Control***). După modelul **HDLC**, standardul **IrLAP** utilizează 3 tipuri de cadre:

- ***Cadre de iniţializare*** (***Unnumbered Frames***) – prin care se stabileşte o conexiune
- ***Cadre cu date*** (***Information Frames***) - care conţin datele

- ***Cadre de comandă*** (***Supervisory Frames***) – care controlează traficul de date

. Pentru transmisiile lente şi transmisiile de viteză se definesc următoarele protocoale:

- ***Asyncron serial IR*** la viteze de ***9,6 Kbps – 115,2 Kbps***
- ***Syncron serial IR*** la viteze de ***576 Kbps – 1,15 Mbps***

- ***Syncron 4PPM*** la viteza de ***4 Mbps***

Conectarea şi transmiterea datelor între două echipamente IrDA se face într-o succesiune de 3 etape (vezi **fig. 1.2.6**):

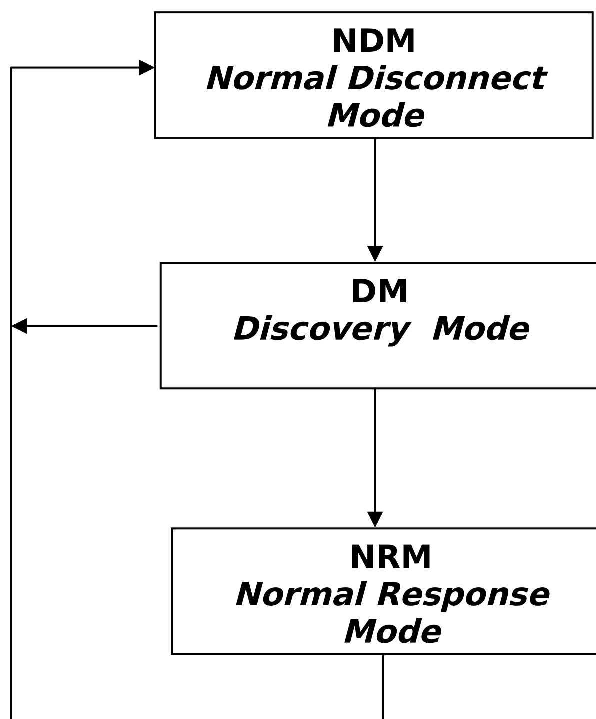


Figura 1.2.6 Etapele de conectare între două echipamente IrDA

- **NDM** (***Normal Disconnect Mode***) – este o stare de aşteptare în care se verifică posibilitatea unei legături. Înainte de a transmite se urmăreşte activitatea mediul. Dacă nu este detectată activitate mai mult de 0,5 s se iniţializează conexiunea.

Dispozitivul primar trimite comenzi de identificare către dispozitivele secundare din raza sa de acţiune.
Dacă un dispozitiv secundar nu este în raza de acţiune a dispozitivului primar sau dacă este ocupat, dispozitivul respectiv nu răspunde.
Dacă un dispozitiv secundar este în raza de acţiune a dispozitivului primar şi nu este ocupat, acesta va răspunde la o comandă a dispozitivului primar.
După ce se identifică, dispozitivul secundar ignoră alte comenzile de identificare trimise de dispozitivul primar.

- **DM** (***Discovery Mode***) – este etapa în care două echipamente IrDA s-au descoperit şi stabilesc parametrii de comunicare.

După ce două dispozitive IrDA s-au identificat, dispozitivul primar trimite către dispozitivul secundar comenzi cu parametrii săi de conectare şi adresa de conectare. Dispozitivul secundar răspunde cu parametrii săi de conectare folosind adresa de conectare specificată de dispozitivul primar.

Dispozitivul primar deschide un canal de interogare a serviciului de acces la informaţii, iar dispozitivul secundar confirmă deschiderea acestui canal.
Dispozitivul primar trimite capacităţile sale cu privire la accesul la informaţii(rata de transfer, dimensiunile pachetelor de date, etc.), iar dispozitivul secundar răspunde cu capacităţile sale de acces la informaţii.
În vederea optimizării performanţelor sistemului, cele două dispozitive vor utiliza capacităţile comune de acces la informaţii.
Dispozitivul primar deschide un canal pentru transmisii de date iar dispozitivul secundar confirmă deschiderea acestui canal şi indică faptul că link-ul este acum deschis şi datele pot fi transmise

- **NRM** (***Normal Response Mode***) – reprezintă modul de operare pentru echipamentele conectate.

După conectare, cele două diapozitive IrDA schimbă între ele date şi informaţii.
După finalizarea comunicării dispozitivul primar închide link-ul de conectare iar dispozitivul secundar confirmă închiderea link-ului.
După închiderea link-ului de comunicare ambele dispozitive revin la starea **NDM**.



AVANTAJELE ŞI DEZAVANTAJELE TEHNOLOGIEI IR

- **AVANTAJE**:
  - dimensiuni mici;
  - puteri mici;
  - nu generează interferenţe electromagmetice (un avantaj major în zonele de lucru cu regim special: centrale nucleare, laboratoare de cercetare);
  - asigură o securitate intrinsecă a datelor.

- **DEZAVANTAJE**:
  - viteze mici de transfer;
  - distanţă mică de transfer;
  - unghi mic de transmitere a datelor.



UTILIZAREA TEHNOLOGIEI IR

Tehnologia IR este ideală pentru conectarea laptop-urilor la următoarele tipurilor de dispozitive:

- Proiector multimedia
- Imprimantă
- Mouse wireless
- Tastatură wireless
- PDA



LIMITĂRILE TEHNOLOGIEI IR

- Semnalele IR sunt afectate de sursele puternice de lumină (în special de iluminatul fluorescent)
- Semnalele IR sunt sensibile la interferenţele electromagnetice.
- Razele IR nu pot trece prin pereţii încăperilor.
- Distanţele dintre laptop-uri şi dispozitivele IR trebuie să fie de maxim 1 m când sunt utilizate pentru comunicaţii şi transferuri de date.



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- sala de clasă
- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea.
- Clasa poate fi organizată frontal sau pe grupe

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe în Power Point pentru prezentarea materialului didactic

- Fişe de lucru pentru elevi



Ca probe de evaluare se pot folosi:

- Probe orale
- Teste scrise

Fişa suport 1.3. Descrierea tehnologiei WAN celulare

Ce?



WAN (*WIDE AREA NETWORK*) – sunt reţele extinse de calculatoare, care acoperă arii geografice mari şi foarte mari şi conectează între ele oraşe, ţări sau continente.

CARACTERISTICILE REŢELELOR WAN:

- Conectează între ele mai multe reţele locale (LAN), facilitând comunicarea între persoane şi computere situate la distanţe mari unele faţă de altele.
- Includ liniile de telecomunicaţii publice cu elementele de legătură şi conectare necesare.
- Utilizează serviciile liniilor telefonice închiriate dedicate acestui scop şi comunicaţiile prin satelit.
- Vitezele de transmisie variază între 1,2 Kbps şi 16 Mbps, iar pentru liniile închiriate şi sistemele bazate pe ATM (***Asynchronous Transfer Mode***) pot ajunge la 156 Mbps.



TEHNOLOGIA WAN CELULARE

Tehnologia WAN pentru telefoane mobile permite accesarea internetului din orice locaţie, mai ales în deplasare, prin intermediul unui adaptor WAN (modem sau telefon celular cu modem inclus) sau a unui card WAN conectat la un dispozitiv mobil.

CARACTERISTICILE REŢELELOR WAN CELULARE:

- Sunt conexiuni wireless de mare viteză ce funcţionează în ambele sensuri.
- Includ trei tipuri de tehnologii:
  - Tehnologii analogice pentru transport de voce;
  - Tehnologii digitale pentru transport de date;
  - Tehnologii de mare viteză pentru transport simultan de voce, video şi date.
- Operează în frecvenţe de 800 MHz şi 1900 MHz.

Un WAN celular permite utilizarea telefonului mobil şi a laptop-ului pentru comunicaţii de tip voce şi date. Pentru a conecta un laptop la o reţea WAN celulară trebuie să utilizaţi un adaptor WAN. Marile companii de telefonie

mobilă: Zapp, Vodafone, Orange, Cosmote pun la dispoziţia utilizatorilor, pe baza unui abonament lunar, adaptoare WAN într-o gamă foarte diversificată(vezi tabelul 1.3.1)

Companie telefonie mobilă	ADAPTOARE WAN
ZAPP	Modemuri: Z020, Z030, Z040, MF 622, MF 626
VODAFONE	USB Stick Huawei 169, Modem 3G Smart
ORANGE	Modem Huawei E270, USB Stick Huawei E870
COSMOTE	Telefoane mobile şi cartele PCMCIA

Tabelul 1.3.1 Adaptoare WAN

MODEMUL Z020

Mod... lans... utilizează serviciul companiei de telefoni... gia CDMA EVDO şi CDMA 1X, care permi... entru download de p... şi de... nentele modemului Z... ate ...

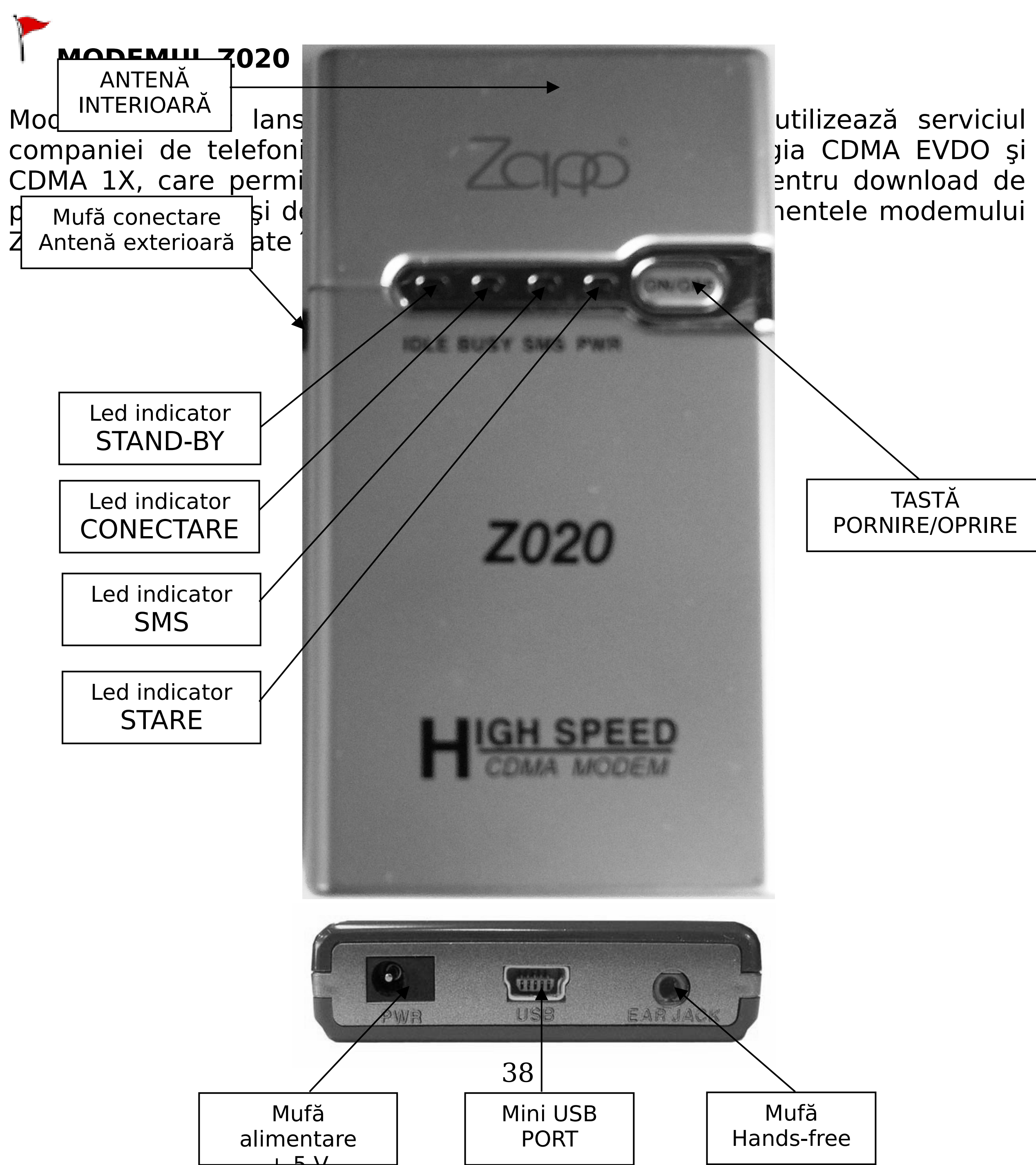


Figura 1.3.1 MODEL DE MODEM

STAREA LED-urilor ŞI INFORMAŢIILE INDICATE DE ACESTEA

- **LED INDICATOR STAND-BY**
  - **ALBASTRU** – Modemul se află în modul de conectare EVDO
  - **INTERMITENT** – Căutare reţea în modul de conectare EVDO
  - **AZURIU** – Modemul se află în modul de conectare HYBRID
  - **INTERMITENT** – Căutare reţea în modul de conectare HYBRID
  - **VERDE** - Modemul se află în modul de conectare CDMA 1X
  - **INTERMITENT** – Căutare reţea în modul de conectare CDMA 1X
  - **STINS** – Modemul este oprit

- **LED INDICATOR CONECTARE**
  - **ALBASTRU** – Conexiune de date în curs
  - **VERDE** – Conexiune de date sau voce în curs
  - **INTERMITENT** – Primire apel voce în curs de conectare
  - **STINS** – Modemul este oprit

- **LED INDICATOR SMS**
  - **GALBEN** – Mesaje primite necitite
  - **INTERMITENT** – Mesaje noi primite
  - **STINS** – Modemul este oprit

- **LED INDICATOR STARE**
  - **ALBASTRU** – Este folosită doar bateria ca sursă de alimentare
  - **INTERMITENT** – Avertizare nivel scăzut al bateriei
  - **ROŞU** – Este folosit numai alimentatorul extern
  - **VIOLET** – Sunt folosite atât alimentatorul extern cât şi bateria
  - **INTERMITENT** – Încărcare în curs
  - **STINS** – Modemul este oprit

Sunt 3 modalităţi de alimentare cu tensiune a modemului:

- De la un alimentator extern care se conectează la mufa de alimentare a modemului
- De la bateria proprie (care se ataşează opţional)
- De la laptop sau PC prin intermediul portului USB prin care modemul se conectează la laptop sau PC

În zonele cu semnal slab, pentru modul de conectare EVDO, trebuie utilizată bateria modemului sau dacă este posibil alimentatorul extern.



INST



1. **Descarc**... /ro-
   drivers.h...
2. **Dezarhiv**...
3. **Conecta**... din
   dotare.
4. **După** co... 3.2
   unde tre... poi
   activaţi l...

Figura 1.3.2

5. După deschiderea ferestrei din figura 1.3.3 activaţi butonului **Browse** şi selectaţi dosarul **Win2K** din locaţia unde a fost dezarhivat fişierul Z020_Driver.zip . Activaţi butonul **Next**.

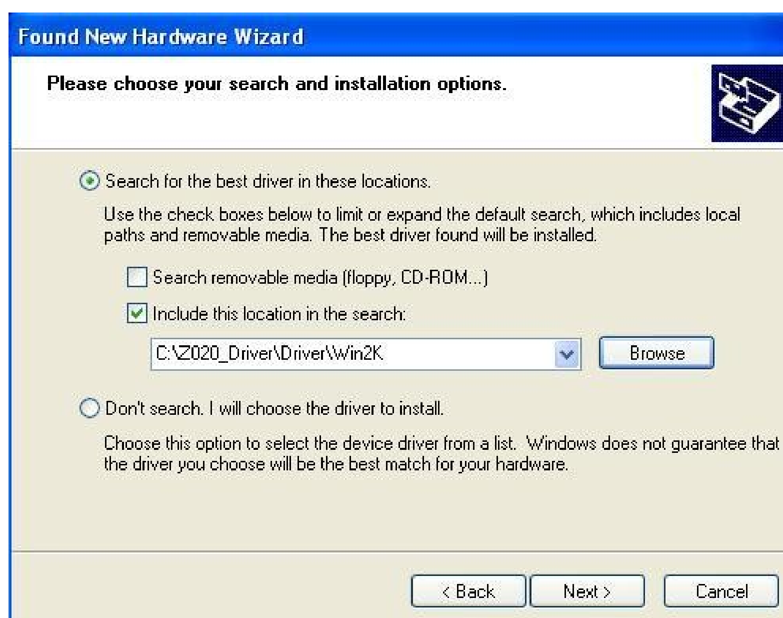


Figura 1.3.3

5. Dupa deschiderea ferestrei din figura 1.3.4, se deschide ferestra din figura 1.3.5 unde trebuie activat butonul **Continue Anyway**

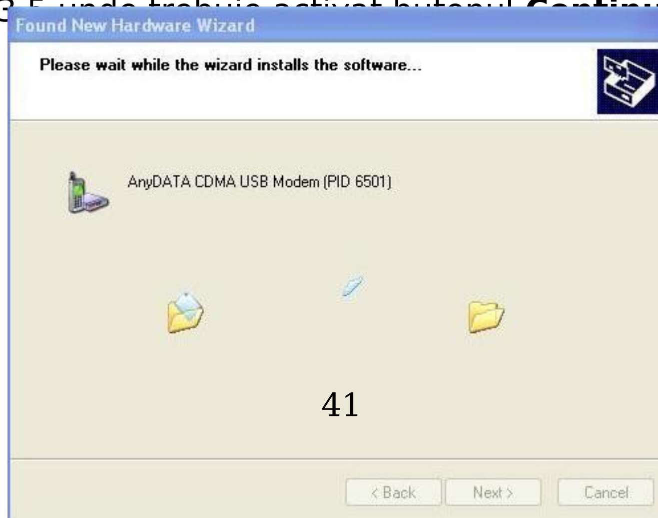


Figura 1.3.4



Figura 1.3.5

6. După finalizarea instalării se deschide ferestra din figura 1.3.6, unde trebuie să activaţi butonul **Finish ,** iar instalarea modemului se finalizeaz



7. După sc .4, moment în care por Parcurgeţi din nou etap le fereastra din figura 1. , iar instalarea portului U



Figura 1.3.7

După finalizarea procedurii de instalare a driverelor verificaţi dacă acestea au fost instalate deschizând ferestra **Device Manager** astfel:

Click cu butonul dreapt al mouse-ului pe **My Computer →** Selectaţi **Properties** din lista care se deschide → În fereastra care se deschide activaţi butonul **Hardware** → Activaţi butonul **Device Manager** şi se deschide fereastra din figura 1.3.8, în care trebuie să apară elementele care sunt subliniate în figură.

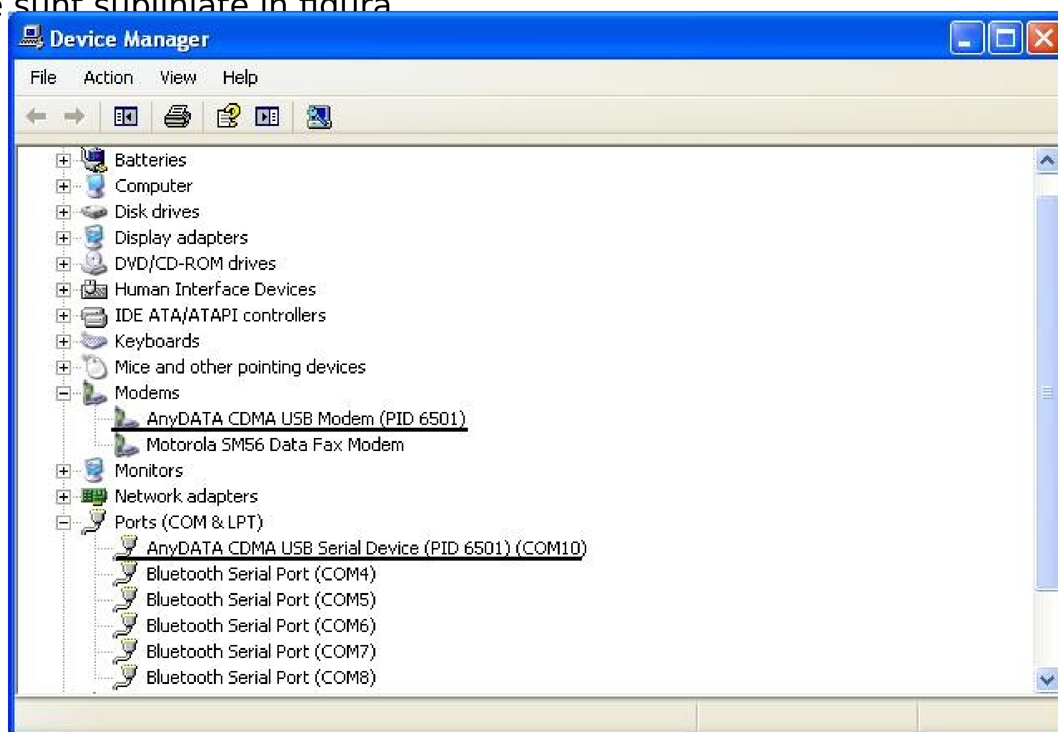


Figura 1.3.8



CREAREA UNEI *CONEXIUNI DIAL-UP*

1. Click cu butonul drept al mouse-ului pe iconul **My Network Place**
2. Din lista care se deschide selectaţi **Properties**

3. În fereastra care se deschide activaţi comanda **Create a new connection**

4. În fereastra care se deschide activaţi butonul **Next**

5. În fereasta **New connection Wizard** din figura 1.3.9 bifaţi opţiunea **Connect to the network at my workplace** apoi activaţi butonul **Next**

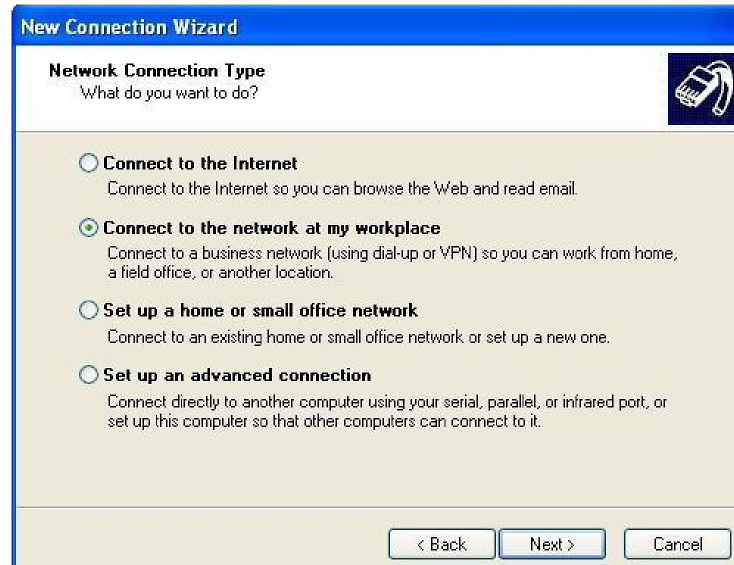


Figura 1.3.9

6. După deschiderea ferestrei din figura 1.3.10, bifaţi **Dial-up connection** apoi activaţi butonul **Next**



Figura 1.3.10

7. După deschiderea ferestrei din figura 1.3.11 bifaţi (dacă nu este bifată) opţiunea **Modem – Any DATA CDMA USB Modem** apoi activaţi butonul **Next**.



Figura 1.3.11

8. După deschiderea ferestrei din figura 1.3.12, în caseta **Company Name** introduceţi un nume pentru conexiune apoi activaţi butonul **Next**



Figura 1.3.12

9. După deschiderea ferestrei din figura 1.3.13, în caseta **Phone number** introduceţi codul **#777** apoi activaţi butonul **Next**

Figura 1.3.13

10. În fereastra care se deschide activaţi butonul **Finish** pentru a finaliza crearea legăturii. După deschiderea automată a ferestrei din figura 1.3.14 , în caseta **User name** introduceţi un nume apoi activaţi butonul **Dial**

Figura 1.3.14

11. Se iniţializează conexiunea şi se va deschide fereastra din figura 1.3.15, unde trebuie să bifaţi **Do not request the failed protocol next time** apoi activaţi butonul **Accept**

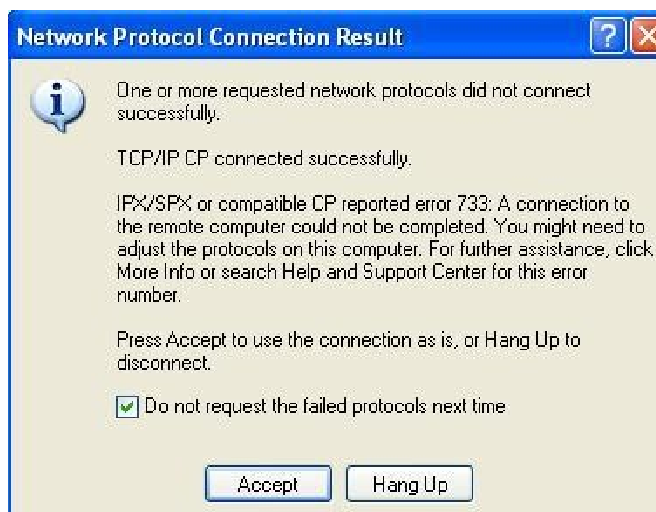


Figura 1.3.15



INSTALAREA PROGRAMULUI *ZAPP INTERNET EXPRESS*

Instalarea acestei aplicaţii se face în cazul în care nu se doreşte crearea conexiunii Dial-up prezentată anterior, situaţie în care conectarea modemului la internet se face prin intermediul aplicaţiei *Zapp Internet Express*. Astfel se poate opta între cele două metode. Pentru instalarea programului *Zapp Internet Express* se parcurg următoarele etape:

1. Descarcărcaţi de la adresa http://www.zappmobile.ro/data/ro-drivers.html fişierul Z020_cd.zip.
2. Dezarhivaţi fişierul, apoi executaţi fişierul **setup.exe** din dosarul în care a fost dezarhivat fişierul Z020_cd.zip

3. După deschiderea ferestrei din figura 1.3.16, selectaţi limba **Română** apoi activaţi butonul **OK**



Figura 1.3.16

4. În fereastra care se deschide activaţi butonul **Inainte**
5. În fereastra care se deschide activaţi butonul **De acord**

6. În fereastra care se deschde activaţi butonul **Instalare**

7. În fereastra care de deschide activaţi butonul **Terminare**

8. După finalizarea instalării se deschide fereastra din figura 1.3.17. Pentru conectarea la internet activaţi butonul **e**





Figura 1.3.17 **Figura 1.3.18**

9. După stabilirea conexiunii se deschide fereastra din figura 1.3.18

10. Pentru deconectarea de la internet activaţi butonul



DESCRIEREA FERESTRELOR APLICAŢIEI ZAPP INTERNET EXPRESS

FEREASTRA PRINCIPALĂ

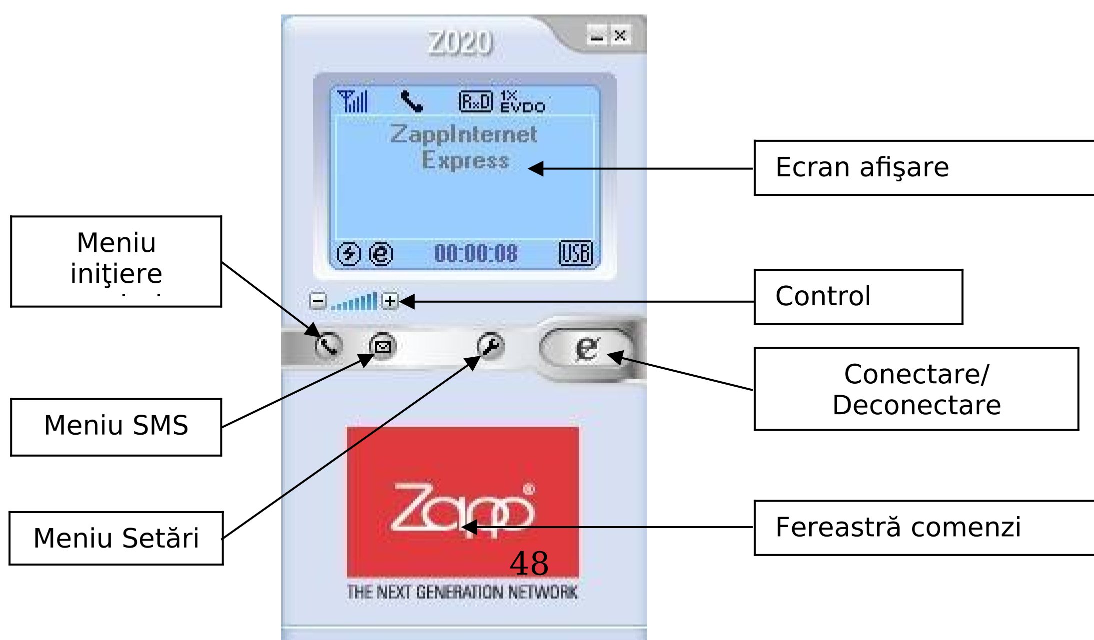


Figura 1.3.19 Interfaţa aplicaţiei Zapp Internet Express

Descrierea pictogramelor

Indicator intensitate semnal

Lipsă semnal

Conectare în modul EVDO

Conectare în modul 1X + EVDO

Conectare în modul 1X

Mod Rx Diversity

Modemul este conectat

Modemul este conectat prin cablu USB

Conexiune la internet activă

MENIUL SETĂRI

Ferestrele meniului **Setări** sun prezentate în figura 1.3.20

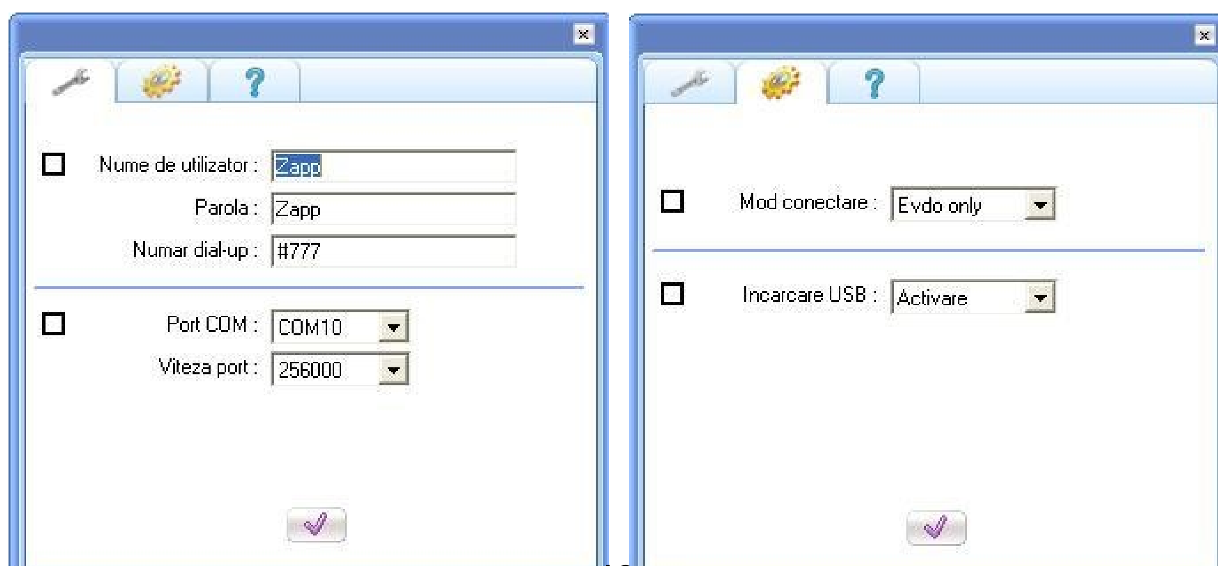


Figura 1.3.20 Ferestrele meniului SETĂRI

Din fereastra din stânga se setează numărul portului şi viteza portului

Din fereastra din dreapta se setează tipul conexiunii:

- În modul **EVDO** viteza de download este până la 2,4 Mbps
- În modul **1X** viteza de download este până la 153,6 Kbps

< NOTĂ> Modemul suportă modul **EVDO** dacă în zonă există acoperire pentru acest mod. Dacă există acoperire şi modemul nu se poate conecta în modul **EVDO** trebuie să conectaţi la modem alimentatorul sau bateria acestuia.

MENIUL SMS

Ferestrele meniului **SMS** sunt prezentate în figura 1.3.21



Figura 1.3.21 Ferestrele meniului SMS



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- sala de clasă
- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea, demonstraţia, experimentul.
- Se pot aplica lecţii de laborator cu tema: **“Instalarea unui adaptor WAN şi accesarea internetului prin intermediul adaptorului respectiv”**
- Clasa poate fi organizată pe grupe de câte 3 – 4 elevi

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic
- Fişe de lucru pentru elevi
- Fişe de laborator
- Adaptoare WAN



Ca probe de evaluare se pot folosi:

- Probe practice

- Probe scrise

Fişa suport 1.4. Descrierea tehnologiei WI-FI

Ce?



WI-FI (***WIRELESS FIDELITY***) – este o tehnologie avansată de conectare într-o reţea WLAN, care utilizează undele radio şi se bazează pe standardele de comunicaţie din familia **IEEE 802.11**.

IEEE (***Institute of Electrical and Electronics Engineers***)- ***Institutul Inginerilor Electrotehnişti şi Electronişti*** este cea mai mare organizaţie de tehnicieni profesionişti din lume, care sprijină evoluţia tehnologiilor bazate pe electricitate.

802.11 este un standard de comunicaţie în reţelele locale, elaborat de IEEE în anul 1990 care în decursul timpului a fost îmbunătăţit şi a apărut în mai multe versiuni:

- **802.11** – a apărut în 1997 (aceast standard astăzi nu mai este utilizat).
- **802.11 a** – a apărut în anul 1999 (nu este compatibil cu celelalte standarde 802.11 x, deoarece foloseşte altă bandă de frecvenţă).
- **802.11 b** – a apărut în anul 1999.
- **802.11 g** – a apărut în anul 2003 (este cel mai utilizat standard la ora actuală).
- **802.11 n** – a apărut în anul 2006, este în fază de proiect şi urmează să fie definitivat în anul 2010.



IEEE 802.11

Standardele din familia **IEEE 802.11** descriu ***protocoalele de comunicaţie*** aflate la ***nivelul fizic*** (**PHY**) şi ***la nivelul legăturii de date*** (**MAC**) ale unei reţelele locale wireless. Stiva de protocoale IEEE 802.11 este prezentată în **figura 1.4.1**. Implementările IEEE 802.11 trebuie să primească pachetele de date de la protocoalele de la nivelul reţea şi să se ocupe cu transmiterea lor evitând eventualele "coliziuni" cu alte staţii din zonă care emit. IEEE 802.11 este compatibil cu Ethernet-ul care este standardizat de IEEE în seria de s

<table>
<tr><td colspan="7">LLC (802.2)</td><td rowspan="2">NIVEL LEGĂTURI DE DATE MAC</td></tr>
<tr><td colspan="4">DCF CSMA/CA MAC</td><td colspan="3">PCF MAC</td></tr>
<tr><td colspan="7">PLCP</td><td rowspan="3">NIVEL FIZIC PHY</td></tr>
<tr><td colspan="7">PMD</td></tr>
<tr><td>Infraroşu</td><td>FHSS</td><td>DSSS</td><td>OFDM (802.11 a)</td><td>HR-DSSS (802.11 b)</td><td>802.11 g</td><td>802.11 n MIMO</td></tr>
</table>

Figura 1.4.1 Stiva protocoalelor IEEE 802.11



WI-FI - NIVELUL FIZIC reprezintă mediile de transmisie wireless a pachetelor de date şi include tehnologiile ce controlează transmisia datelor. Nivelul fizic este format din două subnivele:

- **PMD** (***Physical medium dependent***) – **Subnivelul dependent de mediul fizic** – este echipat cu interfaţă de transmitere şi recepţie a pachetelor de date în mediul wireless
- **PLCP** (***Physical layer convergence protocol***) – **Subnivelul protocolului de convergenţă a nivelului fizic** – este o interfaţă către subnivelul **MAC** (***Media Acces Control***). Subnivelul **MAC** se ocupă de modul cum primesc acces la date calculatoarele din reţea, reprezintă conectivitatea fizică. Subnivelul **PLCP** îndeplineşte funcţia de adaptare a capabilităţilor subnivelului **PMD** la serviciul care trebuie să-l ofere nivelul fizic. **PLCP** defineşte o metodă de includere a unităţilor de date ale protocolului MAC într-un format de cadru adecvat pentru transmiterea şi recepţia datelor de utilizator şi a informaţiei de administrare, între două sau mai multe staţii, utilizând subnivelul **PMD**.

Structura cadrelor PLCP este dependentă de tipul transmisiei, care poate fi:

- **INFRAROŞU** – pachetele de date sunt transmise prin intermediul radiaţiilor electromagnetice din spectrul de lumină infraroşu (vezi fişa suport 1.3).
- **FHSS** (***Frequency-Hopping spread spectrum***) – **Spectru împrăştiat cu salturi de frecvenţă** – pachetele de date sunt transmise prin intermediul undelor radio în banda de 2,4 GHz ISM (vezi fişa support 1.2). Sunt utilizate 79 canale de frecvenţă, fiecare de 1 MHz. Pentru alocarea eficientă a frecvenţelor acestea se schimbă periodic (se sare de la o frecvenţă la alta in mod aleator) în urma unor numere pseudoaleatoare generate de staţiile care comunică.

- **DSSS** (***Direct Sequence Spread Spectrum***) – **Spectru împrăştiat cu frecvenţă directă** – pachetele de date sunt transmise prin intermediul radio în banda de 2,4 GHz ISM. Sunt utilizate 14 canale de frecvenţă, fiecare de 5 MHz.

- **OFDM** (***Orthogonal Frequency Division Multiplexing***) – **Multiplexare cu divizare în frecvenţe ortogonale** – pachetele de date sunt transmise prin intermediul undelor radio, simultan, în paralel,

pe mai multe frecvenţe. Sunt utilizate 52 de canale din care 48 de date şi 4 de sincronizare. Pentru a înţelege sensul termenului de ***frecvenţă ortogonală***, se poate face o analogie între transmiterea unui pachet de date şi un jet de apă care curge print-un robinet(în cazul tehnologiei FDM) sau printr-un duş (în cazul tehnologiei OFDM). Această tehnologie este folosită în banda de 5 GHz pentru 802.11 a şi de 2,4 GHz pentru 802.11 g. Fiecare canal are 300 KHz, iar fiecare utillizator are disponibil 20 MHz. Teoretic viteza de transmisie poate ajunge la 54 Mbps.

- **HR – DSSS** (***High Rate - Direct Sequence Spread Spectrum***) – **Spectru împrăştiat cu frecvenţă directă şi rată ridicată** – este asemănătoare cu tehnologia DSSS, dar cu o rată mai ridicată de transmitere a pachetelor în bandă mai îngustă. Viteza de transmisie ajunge până la 11 Mbps.

- **802.11 g** – este un standard publicat în 2003 de IEEE, care combină banda îngustă a tehnologiei **HR-DSSS** cu tehnica de modulaţie **OFDM**

- **802.11 n** – este un standard adoptat în 2006, care urmează a fi definitivat în 2010. Acesta utilizează tehnologia **MIMO** (***Multiple Input Multiple Output***), care împarte un şir de date în mai multe şiruri şi le transmite simultan, cu viteză mare şi la distanţă mare, folosind mai multe antene. Două şiruri permit o viteză teoretică de maxim 248 Mbps.



WI-FI - NIVELUL LEGĂTURII DE DATE – reprezintă tehnicile de acces ale staţiilor la mediul de transmisie wireless în standardul 802.11

- **DCF** (***Distributed Control Function***) – **Funcţie de Coordonare Distribuită** – este tehnica prin care fiecare staţie controlează propriul acces la mediu, constituind o reţea wireless ad-hoc (vezi **figura 1.4.2**).

Realizarea controlului accesului la mediu se face prin tehnica **CSMA/CA** (***Carrier Sense Multiple Access/Collision Avoidance***) – **Acces aleator cu evitarea coliziunilo**r. Este o tehnică de control al accesului la mediu, care se utilizează în reţelele wireless **pentru a evita coliziunile**. În *eter* coliziunile sunt foarte greu de detectat, de aceea pentru transmiterea datelor IEEE a recurs la această strategie de control al accesului la mediu.

Staţia care transmite cadre MAC ascultă mediul de transmisie. Dacă mediul este ocupat, staţia amână încercarea de a transmite până ce mediul devine liber. Dacă mediul este liber staţia poate transmite . În primul moment al transmisiei staţia trimite un cadru **RTS** (***Request To Send***) şi aşteaptă un răspuns la această cerere. Dacă destinatarul este liber, răspunde cu un **CTS** (***Clear To Send***). După primirea **CTS** staţia transmiţătoare trimite cadrul de date. După transmiterea cadrului se aşteaptă o confirmarea pozitivă pentru a semnala recepţia corectă a cadrului. Dacă nu se semnalează confirmarea pozitivă, cadrul este

retransmis. După o transmisie reuşită staţia trebuie să aleagă un interval de revenire aleatoriu şi să decrementeze controlul intervalului de revenire în timp ce mediul este liber.

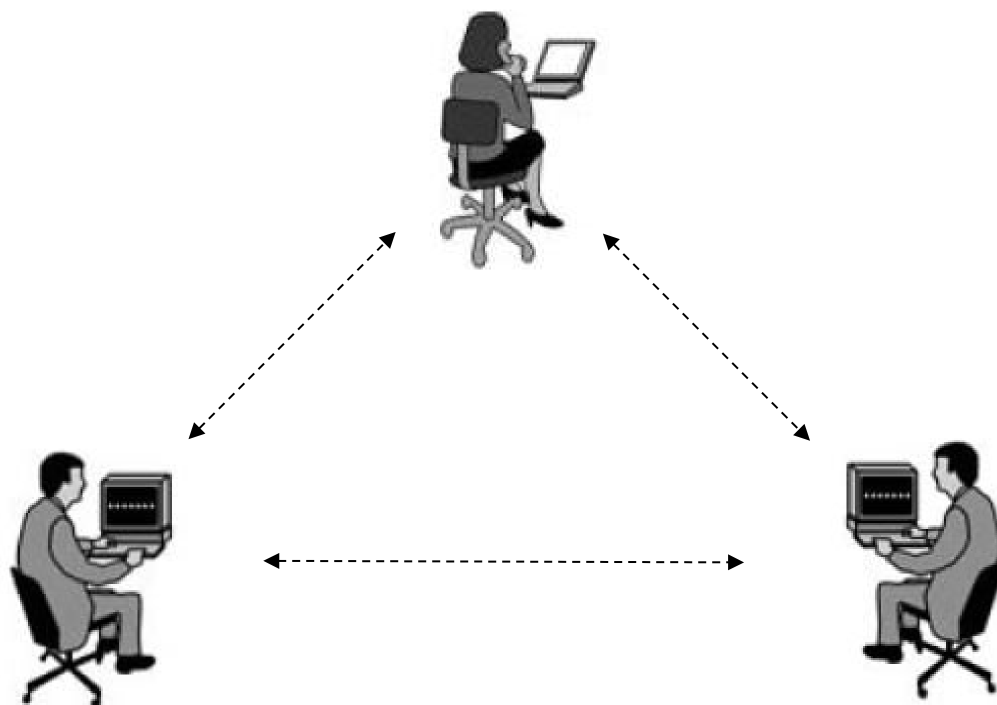


Figura 1.4.2 Re[illegible]***pendent Basic Service Sets***)

- **PCF** (***Point Coordinat***[illegible] – **Funcţie de Coordonare Punctuală** – necesită o [illegible]ată numită **punct de acces** (**AP**) care gestionează accesul la mediu (vezi **figura 1.4.3**). AP este punctul central al comunicaţiei pentru toate celelalte staţii. Staţiile nu pot comunica direct între ele, acestea vor comunica doar când li se permite de către AP. Periodic, staţia de bază (**AP**) emite un cadru care conţine setări privind co[illegible] şi care cere staţiilor ce doresc să se conecteze să anunţ[illegible]

Access Point

Figura 1.4.3 Infrastructura BSS (***Basic Service Sets***)

- **ESS** (***Extended Service S*** ... două funcţii prezentate mai sus (PCF şi DCF), sunt utilizate ... aceeaşi reţea. ESS este un set de două sau mai multe stru... care lucrează împreună pentru a forma o singură reţea ... **.4.4**). Structurile BSS pot fi conectate cu ajutorul un... Interfaţa uplink conectează structurile BSS la un sistem de distribuţie, notat cu DS. Legătura uplink către DS poate fi wired sau wireless.

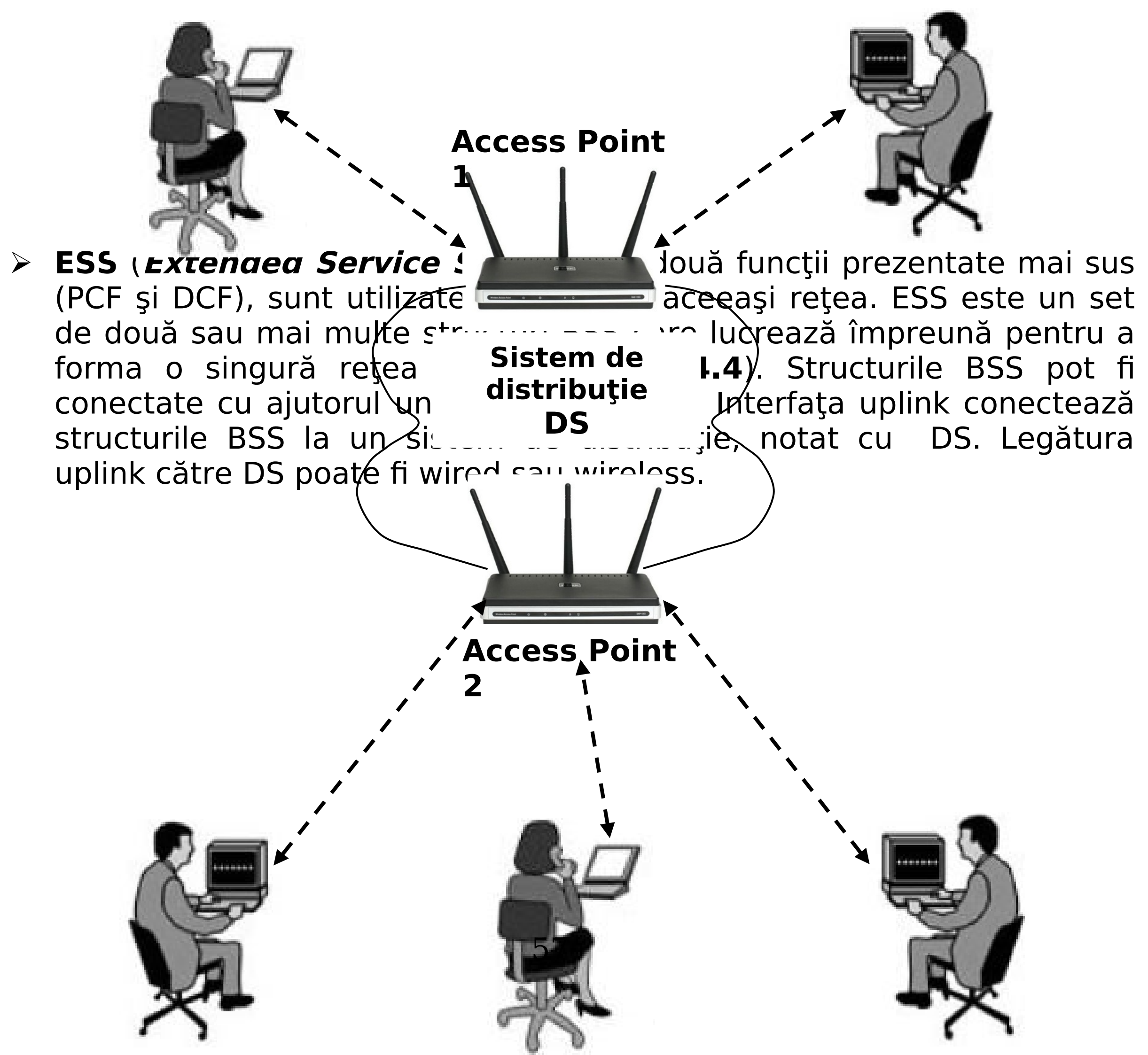


Figura 1.4.4 Infrastructură ESS

- **LLC** (***Logical Link Control***) – **Nivelul logic al legăturii** – este subnivelul care se ocupă cu controlul fluxului de date. IEEE a standardizat LLC sub numele de 802.2 cu mult inainte de elaborarea standardului 802.11. Standardul IEEE 802.2 este utilizat în reţelele Ethernet. Folosirea de către IEEE 802.11 a subnivelului LLC are drept scop realizarea unei tehnologii wireless compatibilă cu tehnologia Ethernet.



SECURITATE WI-FI

Spre deosebire de reţelele cablate, reţelele wireless sunt mai expuse din punct de vedere al vulnerabilutăţii la interceptări neautorizate. La nivel fizic securitatea este greu de asigurat deoarece la acest nivel o reţea wireless este foarte uşor de accesat. Pentru a obţine un nivel de securitate acceptabil, într-o reţea wireless, datele trebuie criptate şi este obligatoriu controlul accesului la nivelurile superioare ale reţelei. Barierele de securitate (securitatea de bază) care au fost prevăzute iniţial în protocoalele reţelelor Wi-Fi, asigură un nivel scăzut al securităţii acestor reţele.

1. Securitate de bază constă în controlarea accesului la reţea prin utilizarea unor tehnici simple, suficiente pentru a îndepărta unele intruziuni ocazionale. Tehnicile simple de control al accesului la o reţea wireless sunt:

- **Filtrarea adreselor MAC** (***Media Acces Control***). Adresa MAC, este un număr întreg pe 6 octeţi (48 biţi), care reprezintă adresa fizică (unică pentru fiecare dispozitiv de acces la o reţea) prin intermediul

căreia orice dispozitiv de acces la o reţea se poate identifica. Prin filtrarea adreselor MAC, un punct de acces în reţea este configurat cu adresele MAC ale clienţilor cărora le este permis accesul în reţea. Această tehnică este ineficientă deoarece un intrus poate afla şi falsifica adresa MAC a unei staţii, apoi se poate conecta în reţea sub identitatea staţiei respective.

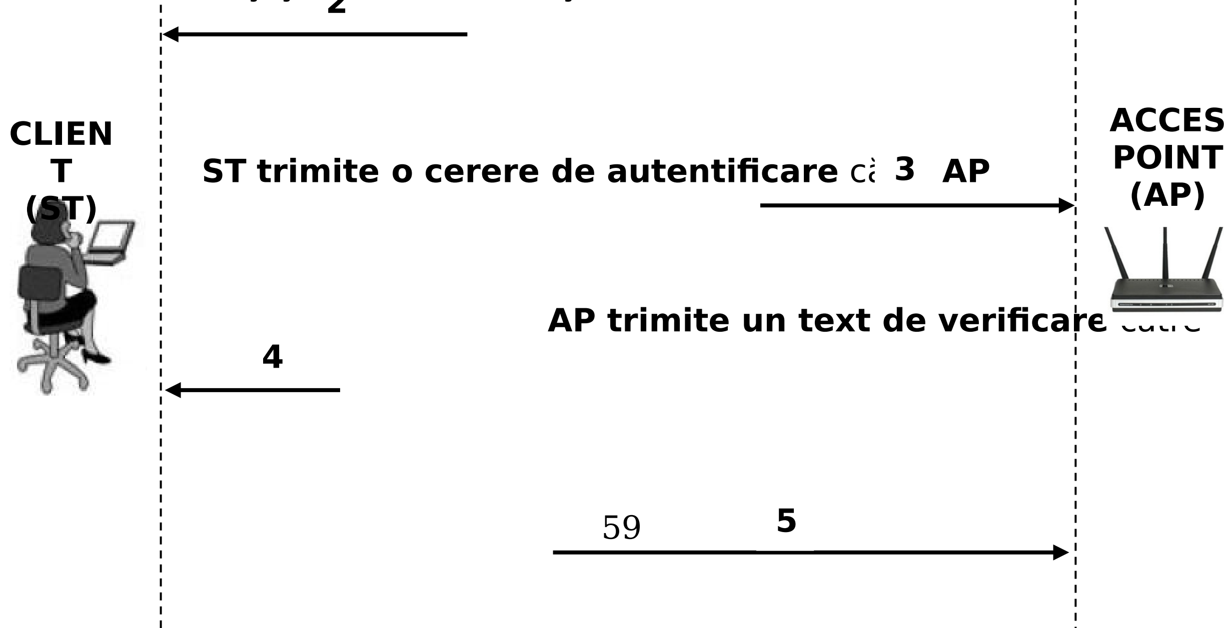
- **Stoparea transmiterii publice a SSID**-ului **unui punct de acces.** SSID-ul (Service Set Identifier) – este un cod care defineşte apartenenţa la un anumit punct de acces wireless. Toate dispozitivele wireless care vor să comunice într-o reţea trebuie să aibă SSID-ul propriu, setat la aceeaşi valoare cu valoarea SSID-ului punctului de acces pentru a se realiza conectivitatea. În mod normal un punct de acces îşi transmite SSID-ul la fiecare câteva secunde. Oprirea transmiterii acestui semnal ascunde prezenţa reţelei faţă de un atacator superficial, dar permite staţiilor care cunosc SSID-ul punctului de acces să se conecteze la reţea. Deoarece SSID-ul este inclus în ***beacon-ul*** oricărei secvenţe wireless, orice hacker dotat cu echipament de monitorizare poate să-i descopere valoarea şi să se conecteze la reţea. **Beacon-ul** este un mic pachet de date transmis continuu de un punct de acces pentru a asigura managementul reţelei.

- **Utilizarea algoritmului WEP** (***Wired Equivalent Privacy***). WEP ameliorează transmiterea continuă a SSID-ului prin criptarea traficului dintre clienţii wireless şi punctul de acces.

  WEP foloseşte un cifru secvenţial **RC4** pentru confidenţialitate şi un **CRC32** pentru integritate în două variante:

  - **64 bit WEP**- foloseşte o cheie de 40 biţi care este concatenată cu un vector de iniţializare de 24 biţi pentru a forma cheia RC4.
  - **128 bit WEP**- foloseşte o cheie de 104 biţi care este concatenată cu un vector de iniţializare de 24 biţi, care este introdusă de utilizator ca un şir hexazecimal format din 26 caractere.

Această tehnică de criptare (vezi **fig.1.4.5**) a fost folosită din anul 1997 până în anul 2001 când a fost spartă şi nu a mai fost considerată sigură. În iunie 2004, IEEE a adoptat standardul 802.11i care îmbunătăţeşte securitatea reţelelor wireless.



ST criptează textul cu o cheie partajată
şi îl trimite înapoi către **AP**

AP decriptează textul şi îl compară cu cel original

Dacă textele corespund, **AP autentifică ST**

ST se conectează la reţea

Figura 1.4.5 Paşii autentificării WEP

În figura 1.4.5 este prezentată **autentificarea prin cheie partajată**. Un alt tip de autentificare pentru standardul IEEE 802.11 este **autentificarea deschisă**.

Autentificarea deschisă se realizează astfel:

- Clientul trimite o cerere de autentificare care conţine ID-ul staţiei (de obicei adresa MAC a plăcii de reţea)

- Punctul de acces verifică ID-ul staţiei şi trimite un răspuns de autentificare care conţine mesajul de succes sau de eşec.

2. Îmbunătăţiri ale securităţii reţelelor wireless.

Wi-Fi Alliance produce în anul 2003 specificaţia **WPA** (***Wi-Fi Protected Access***), care este o soluţie intermediară la criptare WEP.

IEEE a preluat specificaţia WPA şi a elaborat în anul 2004 standardul **802.11i**, standard care stabileşte o tehnică de criptare cunoscută sub numele de **WPA 2**.

- **Algoritmul WPA** – suportă atât autentificare cât şi criptare.

Pentru **autentificare** sunt utilizate două metode:

  - **Autentificare EAP cu standardul 802.1x**:

  EAP (***Extensible Authorization Protocol***) este un cadru de autentificare , o metodă standard pentru autentificarea la o reţea.

  802.1x este un standard de control al accesului la reţea bazat pe porturi, care asigură per utilizator şi per sesiune o autentificare mutuală puternică. Pe baza EAP, 802.1x permite punctului de acces (AP) şi clienţilor din reţea să folosească în comun şi să schimbe chei de autentificare WEP în mod automat şi continuu. Punctul de acces (AP) acţionează ca un proxy server, efectuând cea mai mare parte a calculelor necesare criptării.

  Dacă un utilizator este autentificat prin **802.1x** pentru accesul la reţea, un port virtul este deschis pe punctul de acces (AP) pentru a permite comunicarea. Dacă nu este autorizat cu succes, portul virtual nu este pus la dispoziţie şi comunicarea este blocată. Această metodă de autentificare este mai sigură decât folosirea metodei de autentificare prin utilizarea cheilor pre-partajate.

  - **Autentificarea prin utilizarea cheilor pre-partajate**:

  Prin această metodă, aceeaşi cheie este aplicată atât la cliet cât şi la punctul de acces (AP). WPA foloseşte o metodă care crează o cheie unică pentru fiecare client.

  Pentru **criptare**, s-a păstrat algoritmul de criptare simetrică RC4, dar s-a introdus o tehnică de schimbare a cheii de criptare pe parcursul sesiunii de lucru – **TKIP** (***Temporary Key Integrity Protocol***) şi s-a înlocuit algoritmul de integrare CRC32, utilizat de WPE, cu un nou algoritm numit **Michael**, care este un algoritm de căutare în şiruri de caractere. Acest algoritm foloseşte funcţiile **hash** pentru a găsi un subşir al şirului de căutat. **Funcţiile hash**, numite şi **funcţii de dispersie** sau **funcţii de rezumat**, sunt funcţii definite pe o mulţime cu multe elemente (poate fi o mulţime infinită) cu valori într-o mulţime cu un număr mai mic de elemente(un număr finit de elemente). Una din cerinţele fundamentale pentru o astfel de funcţie este ca, modificând un singur bit la intrare, să producă o avalanşă de modificări în biţii de la ieşire. Funcţiile **hash** sunt utilizate în criptografie, drept componente în schemele de semnătură digitală, formând o clasă de algoritmi criptografici **SHA** (***Secure Hash Algoritm***).

- **Algoritmul WPA 2** – a fost elaborat în anul 2004 de catre IEEE pe baza specificaţiilor algoritmului WPA. În WPA 2 algoritmul de criptare **RC4** este înlocuit cu algoritmul **AES** (***Advanced Encryption Standard***) care este un algoritm standardizat, pentru criptarea simetrică, pe blocuri.

Algoritmul de integrare **Michael** este înlocuit cu mecanismul de criptare **CCMP** (***Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol***) care este bazat pe cifrul **AES**. WPA2 conţine îmbunătăţiri care facilitează roamingul rapid pentru clienţii wireless aflaţi în mişcare. Acest algoritm permite o preautentificare la punctul de acces spre care se deplasează clientul, menţinând în acelaşi timp legătura cu punctul de acces de la care pleacă.

Premisele autentificării WPA 2:

- Punctul de acces **AP** trebuie să se autentifice clientului **ST**
- Trebuie generate chei de criptare

- EAP oferă o cheie de criptare permanentă **PMK** (***Pairwise Master Key***)

- Cu un hash criptografic **SHA** (***Secure Hash Algoritm***) aplicat pe concatenarea: **PMK**; **APnonce**; **STnonce**; **AP_MAC**; **ST_MAC**, este generată cheia **PTK** (***Pairwise Transient Key***)

  * **nonce (number used once)** – un număr aleator folosit o singură dată într-un protocol de autentificare

Paşii autentificării WPA 2 (vezi **figura 1.4.6**):

1. Punctul de acces **AP** trimite către clientul **ST** un **APnonce**;
2. Clientul **ST** generează cheia **PTK**;

3. Clientul **ST** trimite punctului de acces **AP** un **STnonce** împreună cu un cod de intergritate a mesajului (**MIC**) ce include autentificarea;

4. Punctul de acces **AP** generează cheia **GTK**;

5. Punctul de acces **AP** trimite clientului **ST** cheia **GTK** utilizată pentru decriptarea traficului multicast sau broadcast şi un alt **MIC**;

6. Clientul **CT** trimite înapoi către **AP** un mesaj de confirmare **ACK**.

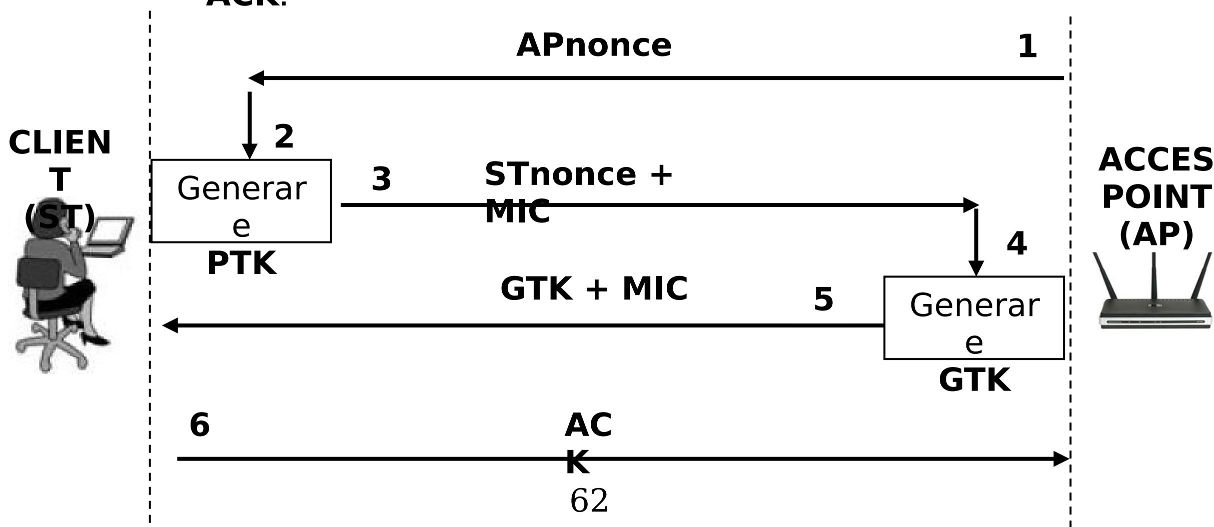


Figura 1.4.6 Paşii autentificării WPA 2

Rezumatul măsurilor de securitate Wi-Fi este prezentat în **figura 1.4.7**

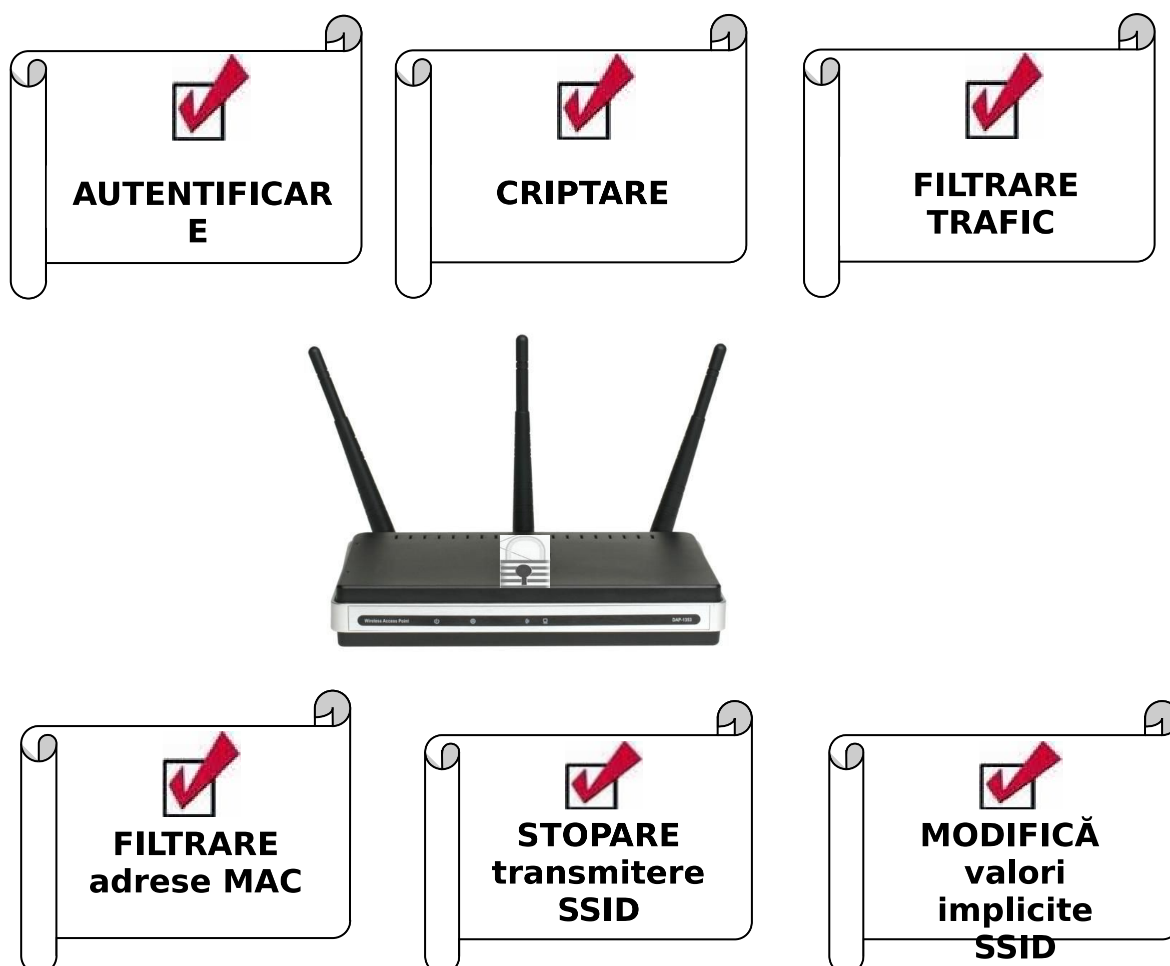


Figura 1.4.7 Măsuri de securitate Wi-Fi



COMPARAŢIE ÎNTRE STANDARDELE 802.11

	802.11 a	802.11 b	802.11 g	802.11 n
Banda [GHz]	**5**	**2,4**	**2,4**	**2,4 5**
Modulaţie	**OFDM**	**DSSS**	**DSSS OFDM**	**MIMO OFDM**

Viteza [Mbps]	**54**	**11**	**11** **54**	**248** **(2 şiruri)**
Distanţa [m]	**max 35**	**35**	**35**	**70**
Anul eliberării	**1999**	**1999**	**2003**	**2006**

TABEL 1.4.1 Standarde 802.11



ECHIPAMENTE Wi-Fi

- **ACCESS POINT** (**figura 1.4.8**) – este un transceiver care transmite şi recepţionează date prin intermediul undelor radio. Acesta permite conectarea dispozitivelor mobile între ele într-o reţea wireless sau poate servii ca punct de interconexiune dintre o reţea wireless şi o reţea LAN. Este prevăzut cu unul sau mai multe conectoare pentru antenă şi un port LAN.



Figura 1.4.8 Access



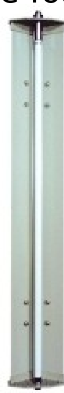
este un dispozitiv de reţea care
s care include şi funcţiile unui
WAN, 4 porturi LAN şi 2 antene



Figura 1.4.9 Router wireless

- **ANTENE WIRELESS** (**figura 1.4.10**) – sunt dispozitive utilizate pentru acoperirea unei anumite zone cu un semnal radio mai puternic. Sunt mai multe tipuri de antene wireless dar cele mai utilizate sunt:
    - **Antene omnidirecţionale** – emit undele radio în toate direcţiile (sferă) şi pot acoperii o suprafaţă cu o rază de 4 – 5 Km. **Avantajul** acestei antene constă în faptul ca antena clientului nu trebuie precis orientată, acesta trebuie doar să se afle în aria de acoperire a antenei staţiei care emite. **Dezavantajul** acestei antene este securitatea scăzută datorită riscului ridicat de interceptare a undelor radio.
    - **Antene sectoriale** – sunt antene omnidirecţionale cu suprafaţă de acoperire mare
    - **Antene direcţionale** – emit şi concentrează undele radio pe o anumită direcţie în funcţie de orientarea antenei. Cu cât unghiul de emisie este mai mic, cu atât distanţa de emisie este mai mare. **Avantajul** acestei antene este riscul scăzut de interceptare a undelor radio. **Dezavantajul** acestei antene este ... :ului trebuie foarte precis







Antenă omnidirecţională Antenă sectorială Antenă direcţională

Figura 1.4.10 Antene wireless

- **Splitter** (**figura 1.4.11 a**) – este un conector utilizat pentru conectarea la un access point a doua antene
- **Pig tail** (**figura 1.4.11 b**) – este un cablu care conectează două echipamente wireless şi care are conectori diferiţi la ambele capete. Se poate utiliza pentru conectarea unei placi wireless la o antenă.

- **Surge protector** (**figura 1.4.11 c**) – este un dispozitiv care protejează AP când un fulger loveşte antena. Acest dispozitiv trebuie conectat la pământ.







a **b** **c**

Figura 1.4.11 Accesorii wireless



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- sala de clasă
- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea.
- Clasa poate fi organizată frontal sau pe grupe

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic

- Fişe de lucru pentru elevi

- Echipamente Wi-Fi

 **Ca probe de evaluare** se pot folosi:

- Probe orale
- Teste scrise

Fişa suport 1.5. Descrierea tehnologiei satelit

Ce?



SATELIŢII ARTIFICIALI – sunt nave robotizate create de om, care sunt lansate în spaţiu şi orbitează în jurul pamântului sau a altor corpuri cereşti.

În funcţie de parametrii lor orbitali sateliţii artificiali se împart în 3 categorii:

- Sateliţi **GEO** (***Geostationary Earth Orbit***) – au orbita în plan ecuatorial, situaţi la 36000 Km de suprafaţa Pământului şi se rotesc sincron cu acesta.
- Sateliţi **MEO** (***Medium Earth Orbit***) – au orbită medie, situaţi la 1500-36000 Km de suprafaţa Pământului.
- Sateliţi **LEO** (***Low Earth Orbit***) – au orbită joasă, situaţi la 500-1500 Km de suprafaţa Pământului.

În funcţie de domeniul de utilizare sateliţii artificiali pot fi:

- **Sateliţi de telecomunicaţii** – utilizaţi pentru transportul undelor radio, tv şi a semnalelor telefonice pe distanţe foarte mari.
- **Sateliţi de navigare** – utilazaţi pentru localizarea navelor şi a mijloacelor de transport echipate cu **GPS** (***Global Positioning System***).
- **Sateliţi meteorologici** – utilizaţi pentru colectarea datelor privind prognoza meteo pe termen lung.
- **Sateliţi militari** – utilizaţi pentru transmiterea datelor codificate între locaţiile militare.
- **Sateliţi ştiinţifici** – utilizaţi pentru studierea Pământului şi a altor corpuri cereşti.



SATELIŢII DE TELECOMUNICAŢII – **ComSat** (***Communication Satellite***) –fac posibilă realizarea unor canale de telecomunicaţii. Sunt întrebuinţaţi aproape în toate domeniile comunicaţiilor: telefonie, televiziune, radio, internet, transmisii de date, videoconferinţe, etc. Sateliţii de telecomunicaţii sunt de două tipuri:

- **Activi** – echipaţi cu aparatură de recepţie-emisie, efectuând anumite modificări asupra semnalului primit

- **Pasivi** – retransmit semnalele primite în urma reflexiei acestora de suprafaţa lor.

Avantajele majore ale sateliţilor de telecomunicaţii sunt:

- **Acoperire foarte mare**, chiar globală, a serviciilor.
- **Comunicaţii mobile** către vase, avioane.

- **Lipsa obstacolelor** în calea undelor transmise sau recepţionate.

Componentele de bază ale sateliţilor de telecomunicaţii (vezi **fig.1.5.1**)

- **ANTENA PARABOLICĂ** – este un reflector metalic de forma unei porţiuni dintr-un paraboloid de rotaţie. Fascicolul undelor electromagnetice recepţionat de parabolă este reflectat şi concentrat în focarul parabolei, de unde este preluat şi prelucrat de un convertor (în cazul **recepţiei semnalului**). Parabola transformă undele sferice emise de convertorul din focar, în unde plane, realizând o caracteristică de radiaţie cu o pronunţată directivitate de-a lungul axei paraboloidului (în cazul **transmisiei semnalului**). Un satelit de telecomunicaţii este prevăzut cu mai multe antene:

  1. **Antenă parabolică de transmisie**

  2. **Antenă parabolică de recepţie**

  3. **Antene parabolice reflectoare**

  4. **Antenă omnidirecţională**

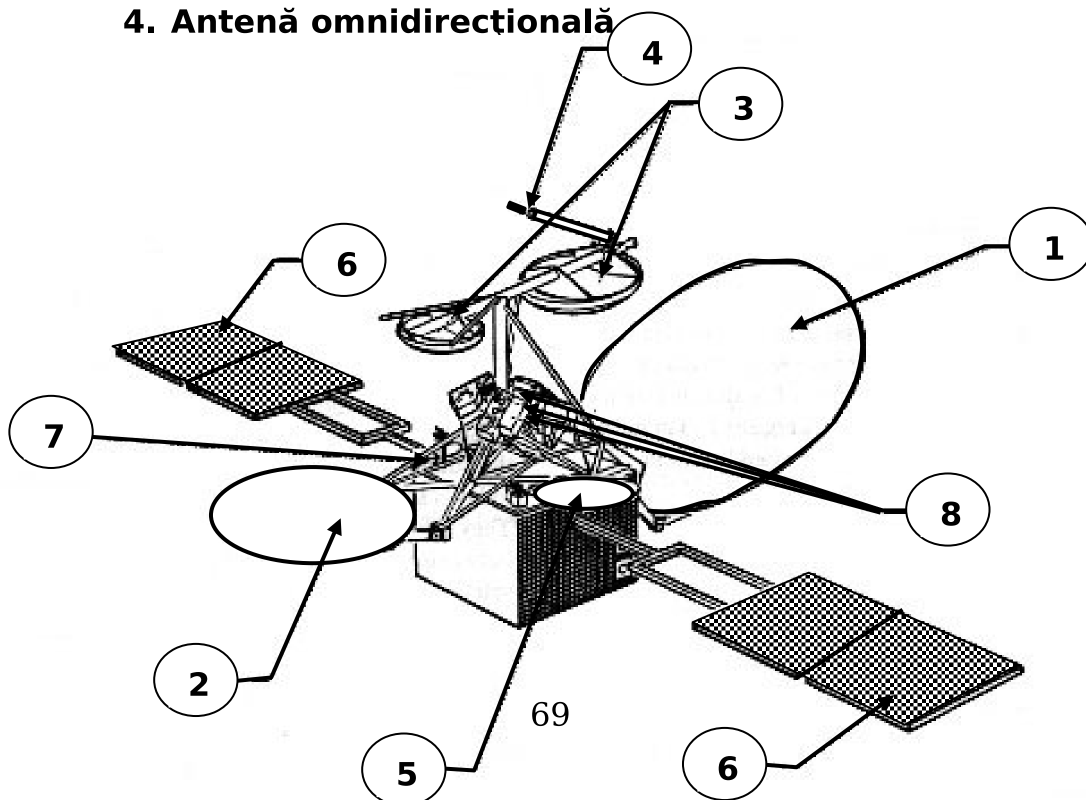


Figura 1.5.1 Componentele de bază ale unui satelit de telecomunicaţii

 **INTERNET PRIN SATELIT** – este un serviciu utilizat în locaţiile terestre în care accesul la internet nu este disponibil şi în locaţiile care sunt în mişcare în mod frecvent. Pentru accesarea internetului se utilizează sateliţi de telecomunicaţii. Pachetele de date circulă pe două căi:

- **Uplink** – datele sunt transmise dinspre Pământ spre satelit
- **Downlink** – datele sunt transmise de la satelit spre Pământ

Există 3 tipuri de acces la internet prin satelit:

- Acces **one – way** – foarte puţin interactiv, deoarece nu permite răspuns din partea utilizatorului.
- Acces **one – way cu răspuns terestru** – o combinaţie între serviciile internet via satelit şi serviciile internet via cablu. Servciul internet via cablu este utilizat pentru transmiterea datelor spre satelit (**uplink**) prin intermediul unei linii telefonice închiriare sau dial-up. Serviciul internet via satelit este utilizat pentru recepţioanarea datelor transmise de satelit (**downlink**)

- Acces **two – way** – acces interactiv la internet direct prin satelit. Utilizează căi de date cu 2 direcţii. Un canal este utilizat pentru transmiterea datelor spre satelit (**uplink**) iar celălalt canal este utilizat pentru recepţionarea datelor transmise de satelit (**downlink**).

Serviciul one – way – este utilizat de persoane particulare, şcoli, diverse instituţii şi firme care deţin o legătură la internet dar care nu eate suficient de rapidă pentru nevoile lor. Legătură la internet este utilizată pentru **uplink** prin care se transmite internetului ce se doreşte, iar prin instalaţia de satelit se realizează **downlink-ul** prin care internetul răspunde cu o viteză de 15-30 ori mai mare decât în cazul unei legături dial-up.

Echipamentele necesare pentru implementarea acestui serviciu sunt:

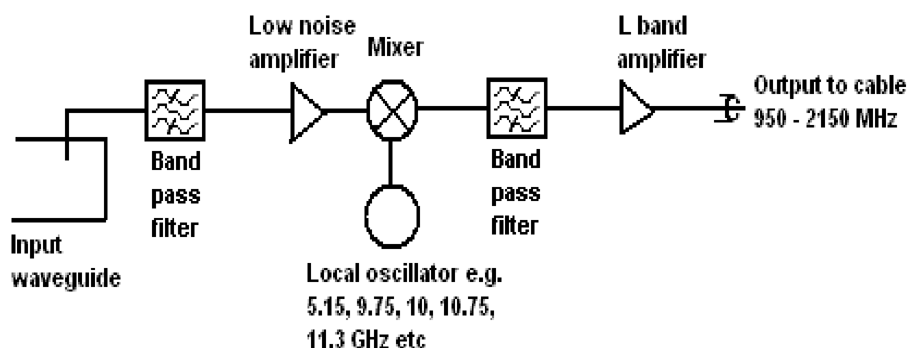
- **ANTENĂ DE SATELIT +LNB** (**figura 1.5.2**)



Figura 1.5.2 Antenă de satelit + LNB

  - **Antenă de satelit** – este o antenă parabolică care recepţionează pachetele de date transmise de satelit
  - **LNB** (**Low Noise Block)** (vezi **fig.1.5.3**) – este un convertor, plasat în focarul antenei parabolice, care are rolul de a amplifica semnalul primit de la satelit si a converti frecventa semnalului din banda 10,7 – 12,8 GHz în banda 950 – 2150 MHz.





a) LNB **b) Schemă bloc LNB**

Figura 1.5.3 Convertor LNB

- **DBV**(***Digital Video Broadcasting***) (vezi **fig. 1.5.3**) – este un dispozitiv care conţine un receiver digital şi un modem satelit, care recepţionează serviciile de date digitale transmise prin satelit. Placa se conectează la convertorul **LNB** din focarul antenei parabolice prin intermediul unui cablu coaxial.



Figura 1.5.3 Placă DVB

- **Serverul de satelit** – asigură navigarea pe internet şi download-ul prin intermediul satelitului. Serverul este conectat printr-o reţea **VPN** (***Virtual Private Network***) împreună cu serverul reţelei locale la internet. Conţine şi placa **DBV**.

Implementarea serviciului one – way (vezi **fig. 1.5.4**)

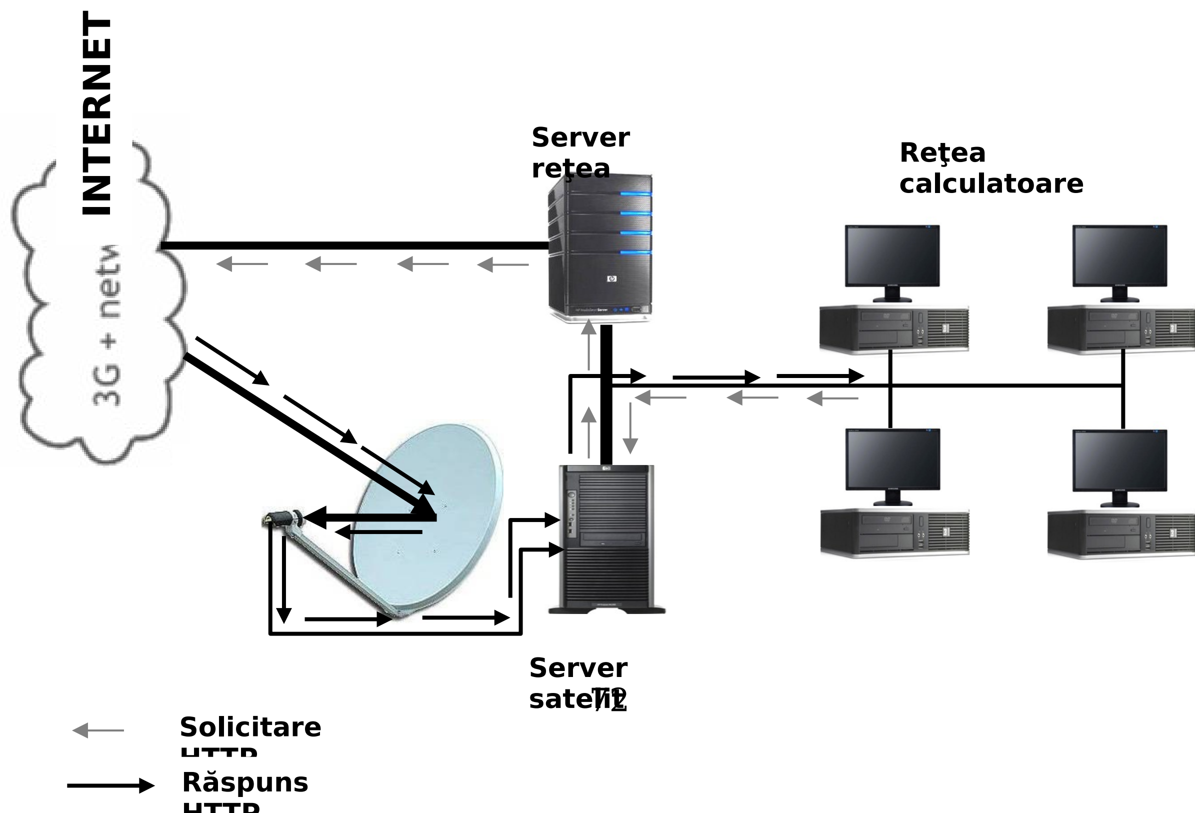


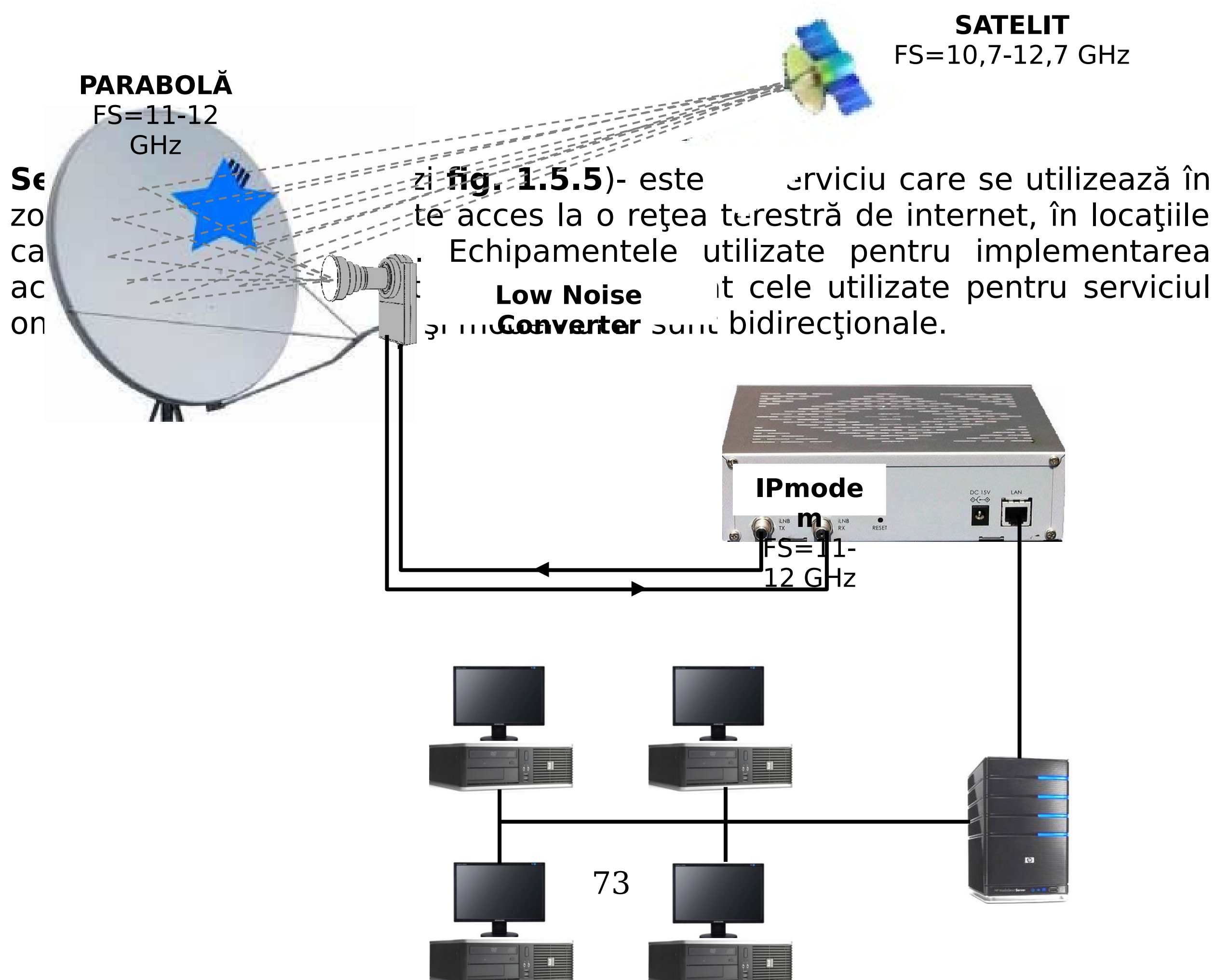
Figura 1.5.4 Reţea cu serviciul ONE WAY

Când un calculator din reţea solicită informaţii, această solicitare este transmisă **serverului satelit**. Serverul satelit retransmite solicitarea **serverului de reţea** şi prin intermediul unei linii telefonice închiriate sau dial-up către **internet.**

Informaţiile solicitate sunt trimise prin intermediul antenei de satelit către serverul satelit care îl trimite mai departe solicitantului.

Prin intermediul liniei telefonice închiriate se solicită de catre un calculator accesarea unei pagini WEB din internet, iar prin intermediul antenei parabolice se recepţionează pagina respectivă şi se face download.

Traficul de mesaje e-mail şi chat-ul se face numai prin intermediul liniei telefonice închiriate sau dial-up, fără a mai trece prin serverul satelit.



Se… zi **fig. 1.5.5**)- este … erviciu care se utilizează în zo… te acces la o reţea terestră de internet, în locaţiile ca… . Echipamentele utilizate pentru implementarea ac… t cele utilizate pentru serviciul on… şi … sunt bidirecţionale.

Figura 1.5.5 Reţea cu serviciul TWO WAY



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- sala de clasă
- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea.

- Clasa poate fi organizată frontal sau pe grupe

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic
- Fişe de lucru pentru elevi

**Ca probe de evaluare** se pot folosi:

- Probe orale
- Teste scrise

Tema 2. Realizarea unei reţele de comunicaţii folosind una din metodele de comunicaţie wireless

Fişa suport 2.1. Realizarea unei reţele wireless ad/hoc (point to point)



Pentru realizarea unei reţele wireless între două laptop-uri, cu scopul transferului de date între cele două laptop-uri, parcurgeţi următoarele etape:

A. Creaţi reţeaua wireless pe unul din laptop-uri astfel:

1. Activaţi serviciul wireless prin apasarea simultană a t **Fn** şi a tastei **funcţionale** pe care se află simbolul wireless

2. Activaţi placa de reţea wireless astfel: click cu butonul drept al mouse-ului pe iconul **My Network Place** → din lista derulantă care se deschide activaţi **Properties** → în fereastra care se deschide (figura 2.1.1) faceţi click cu butonul drept al mouse-ului pe **Wireless Network Connection** → din lista derulantă selectaţi **Enable**.

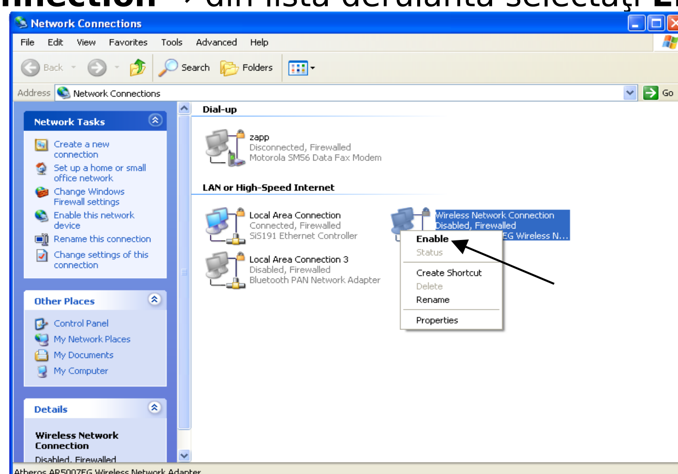


Figura 2.1.1

Placa de reţea este activă dacă în bara tray icon apare iconul: 
Figura 2.1.2

Dacă iconul nu apare deschideţi din nou ferestra **Network Connection** şi observaţi dacă iconul reţelei wireless este activ.



Figura 2.1.3

Dacă iconul este activ faceţi click cu butonul drept al mouse-ului pe icon iar din lista derulantă selectaţi **Properties**. În următoarea fereastră care se deschide verificaţi dacă este bifat ***Show icon in notification area when connected***.

3. Faceţi dublu click cu butonul stâng la mouse-ului pe iconul reţelei wireless din tray icon şi se va deschide fereastra **Wireless Network Connection** (fig. 2.1.4)

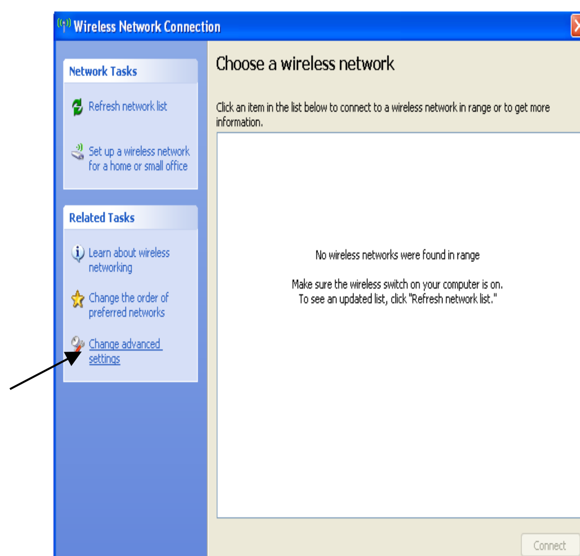


Figura 2.1.4

4. Activaţi comanda **Change advanced settings** din figura 2.1.4 şi se va deschide fereastra **Wireless Network Connection Properties** (figura 2.1.5)

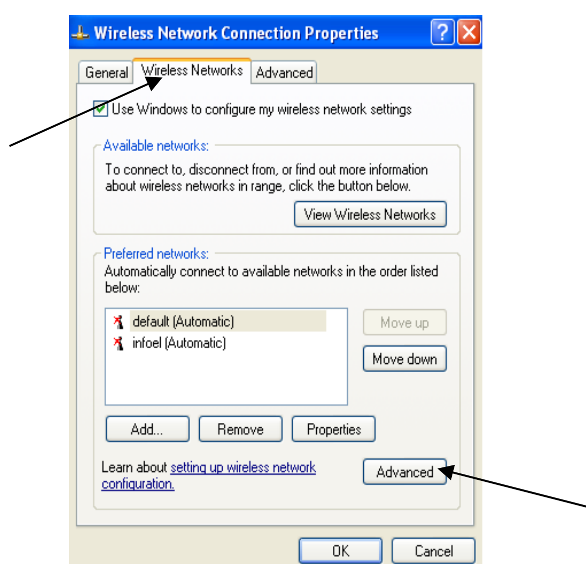


Figura 2.1.5

5. Activaţi butonul **Wireless Networks**, apoi butonul **Advanced** după cum este prezentat cu săgeţi în figura 2.1.5 şi se va deschide fereastra din figura 2.1.6

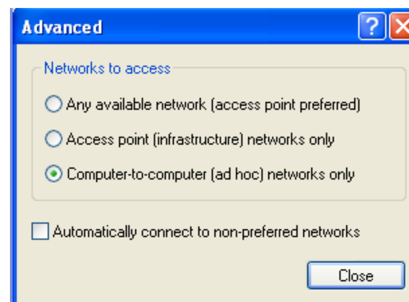


Figura 2.1.6

6. În fereastra **Advanced** bifaţi **Computer-to-computer (ad hoc)** după care închideţi ferestra şi activaţi butonul **Add...** după cum este arătat în ferestra din figura 2.1.7

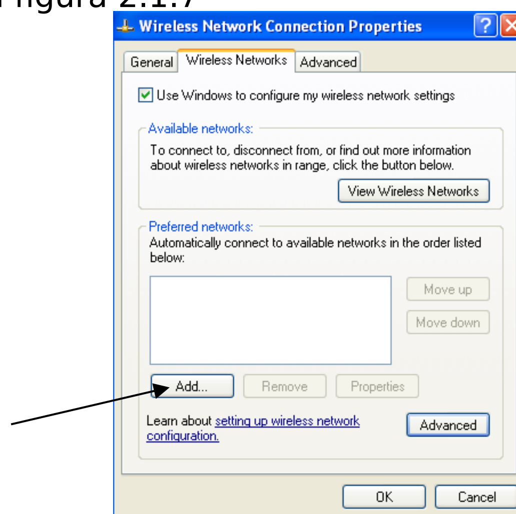


Figura 2.1.7

7. După activarea butonului **Add...** se va deschide ferestra **Wireless network properties** (figura 2.1.8)

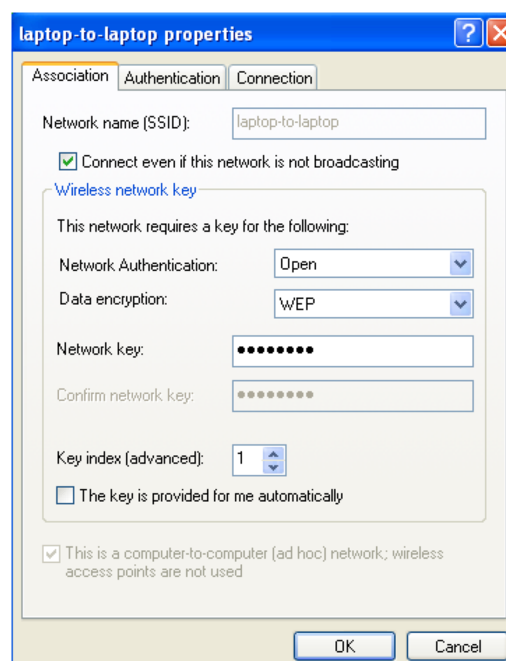


Figura 2.1.8

8. În fereastra care s-a deschis procedaţi astfel:

- În caseta **Network name(SSID)** scrieţi un nume pentru reţea
- Bifaţi opţiunea **Connect even if this network is not broadcasting**
- În caseta **Network Authentication** rămâne **Open**
- În caseta **Data encryption** rămâne **WEP**
- Debifaţi **The Key is provided for me automatically**
- În caseta **Network key** scrieţi o parolă din cel puţin 10 caractere
- Activaţi butonul **OK**

9. Se deschide automat fereastra din figura 2.1.9, în care verificaţi numele reţelei

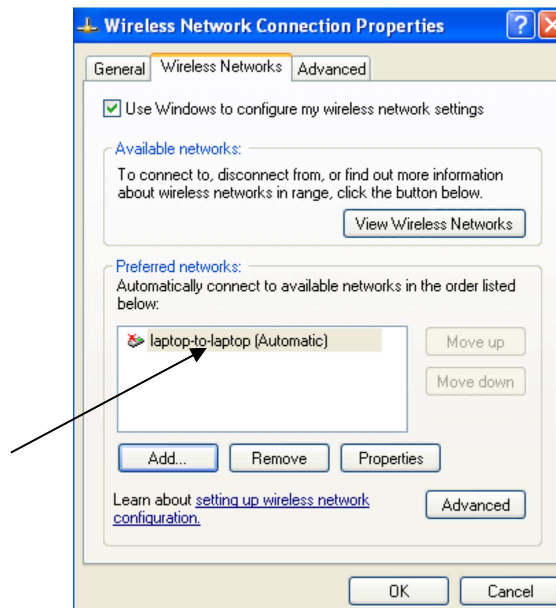


Figura 2.1.9

10. Activaţi butonul **OK**

După ce aţi creat reţeaua wireles treceţi la următoarea etapă de conectare a laptop-urilor la reţea

B. Conectaţ

1. Pe al doilea l fereastra care se deschide (fig

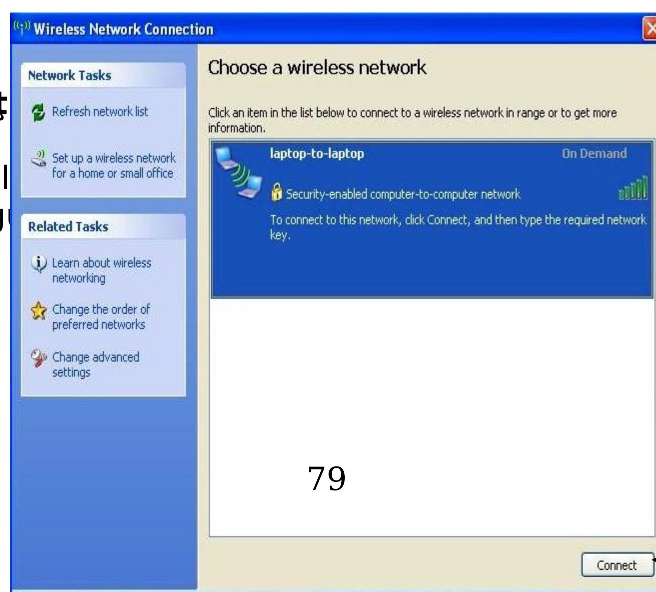


Figura 2.1.10

2. După apăsarea butonului **Connect** se deschide fereastra din figura 2.1.11, ia[...] de la punctul **8** etapa **A**

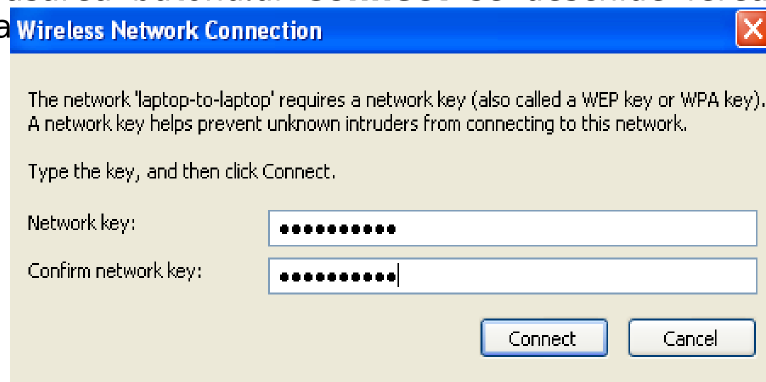


Figura 2.1.11

3. După ce aţi introdus aceeaşi p[...] [...]bele casete, activaţi butonul **Connect** şi aşteptaţi să se realizeze conexiunea. După realizarea conexiunii iconul reţelei wireless din tray icon arată astfel

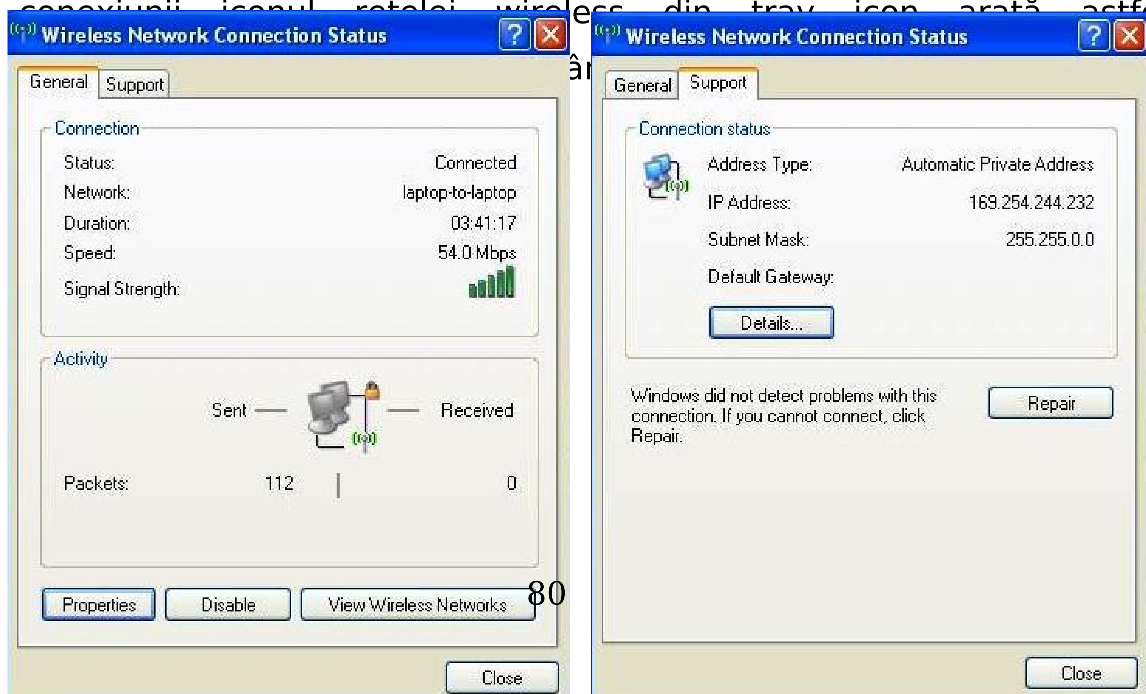


Figura 2.1.12 **Figura 2.1.13**

4. Dacă se activează butonul **Support** din fereastra care este prezentată în figura 2.1.12, se deschide fereastra din figura 2.1.13, unde se observă că laptop-ului ia fost alocată automat adresă de **IP**.

5. După conectarea celui de-al doilea laptop la reţea, se observă că primul laptop, pe care s-a creeat reţeaua se va conecta automat la reţea (figura 2.1.14)

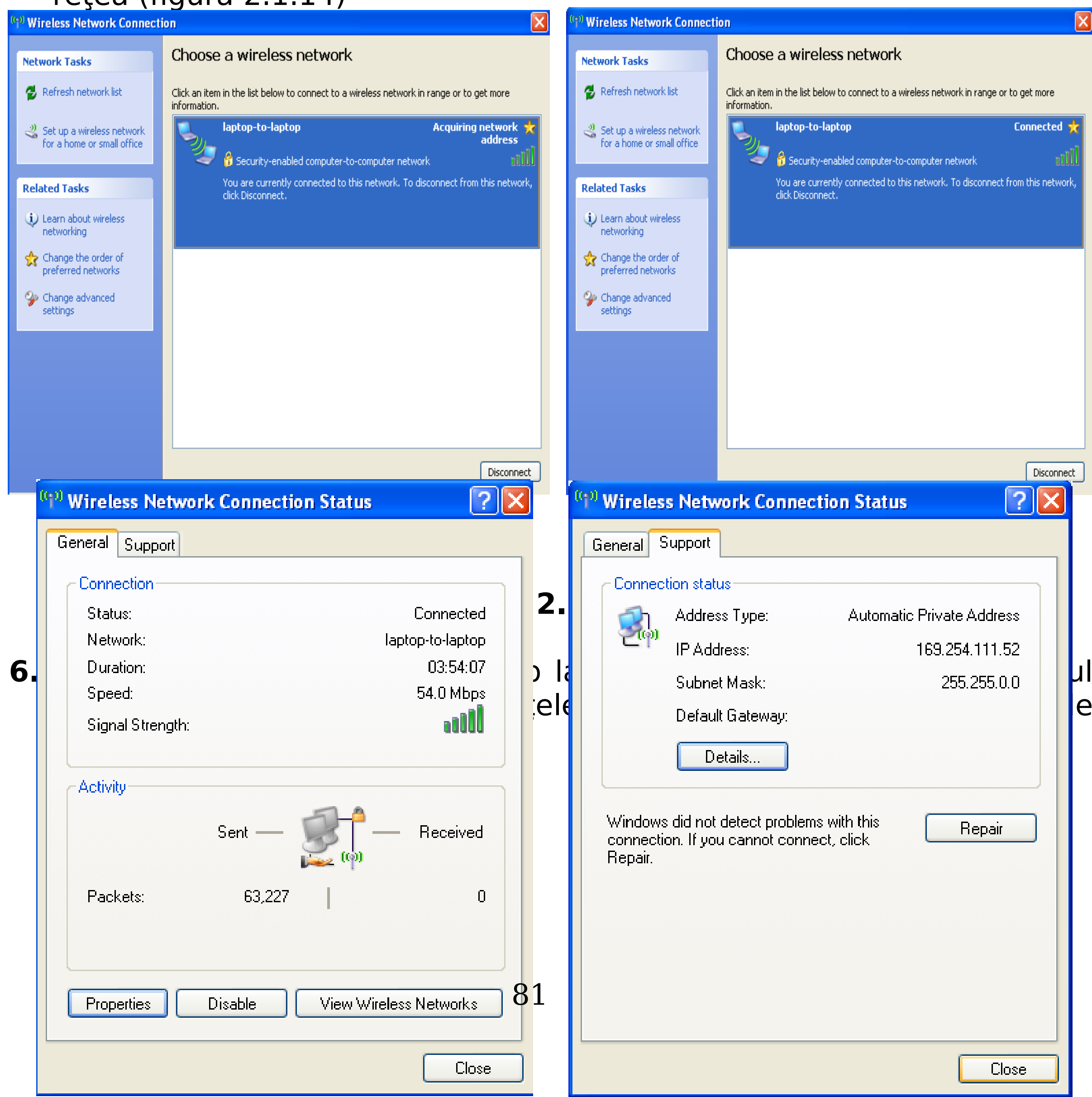


Figura 2.1.15 **Figura 2.1.16**

7. Butonul **Support** (figura 2.1.16), oferă informaţii despre adresa **IP** alocată laptop-ului.

Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea, demonstraţia, experimentul.
- Se aplică lecţii de laborator cu tema: **" Crearea unei reţele wireless ad-hoc"**
- Clasa poate fi organizată pe grupe de câte 2 elevi

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic
- Fişe de laborator
- Laptop-uri şi PC-uri prevăzute cu plăci de reţea wireless



Ca probe de evaluare se pot folosi:

- Probe practice

Fişa suport 2.2. Realizarea unei reţele wireless infrastructure (Access Point)

În modul **Infrastructure**, fluxul de date este gestionat de un echipament wireless numit **access-point**, care poate realiza şi legătura cu reţeaua cablată.



Pentru realizarea unei reţele wireless cu Access Point, cu scopul conectării a două sau mai multe laptop-uri la internet, parcurgeţi următoarele etape:

A. Realizaţi setările de bază (parametrii conexiunii radio) în Access Point, parcurgând următorii paşi:

- Conectaţi dispozitivul Access Point la un laptop. Portul LAN al dispozitivului Access Point se conectează la portul LAN al laptop-ului prin intermediul unui cablu FTP sau UTP prevăzut la ambele capete cu conectori RJ-45.

- Setaţi placa de reţea a laptopului cu un IP static din clasa IP. Această clasă este specificată în documentaţia AP (în cazul nostru **192.168.0.2**):

Click cu butonul drept al mouse-ului pe iconul My Network Place→ Properties→ Click cu butonul drept al mouse-ului pe iconul placii de reţea→ Properties→ Selectaţi Internet Protocol (TCP/IP)→ Activaţi butonul Properties→ se deschide fereastra din figura 2.2.1

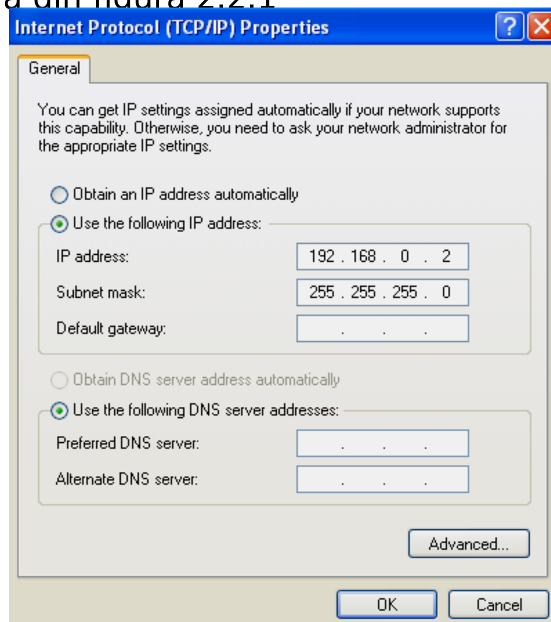


Figura 2.2.1

În fereastra astfel deschisă bifaţi **Use the following IP address** iar în caseta **IP address** completaţi adresa **192.168.0.2** după care apăsaţi butonul **OK**.

- Resetaţi dispozitivul Access Point (ţineţi apăsat butonul RESET 10 secunde)

- Deschideţi pe laptop aplicaţia **Internet Explorer** iar în bara de adrese treceţi adresa AP (**http://192.168.0.1**) apoi apăsaţi tasta **ENTER**.

- Se deschide fereastra din figura 2.2.2, unde în caseta **User name** introduceţi user name-ul (în cazul nostru **admin**) iar în caseta **Password** introduceţi parola (in cazul nostru **admin**), apoi activaţi butonul **OK**



Figura 2.2.2



Figura 2.2.3

- În lista de meniuri din stânga al ferestrei din figura 2.2.3 selectaţi **Wireless Setting** şi se deschide fereastra din figura 2.2.4

Wireless Setting

This page allows you to define Alias Name, ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	AP
Alias Name :	Wireless AP
ESSID :	Wireless cu Acces Point
Channel Number :	11
Associated Clients :	Show Active Clients

Apply Cancel

Figura 2.2.4

- În caseta **Mode** se selectează tipul reţelei (in cazul acesta **AP**)

  În caseta **ESSID** se trece numele reţelei

  În caseta **Channel Number** se selectează unul din cele 13 canele disponibile pentru Europa

- Activaţi butonul **Apply**
- Pentru securizarea reţelei în meniul din stânga al ferestrei din figura 2.2.3 selectaţi **Security** şi se deschide fereastra din figura 2.2.5

Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption :	WPA pre-shared key
WPA Unicast Cipher Suite :	TKIP AES
Pre-shared Key Format :	Passphrase
Pre-shared Key :	AAAAAAAAAA

Apply Cancel

Figura 2.2.5

- În caseta **Encryption** treceţi modul de securizare (WEP, WPA, etc.)

  În caseta **Pre-shared Key** treceţi o parola care trebuie sa aibă cel puţin 8 caractere. Dacă doriţi ca această parolă să conţină cel putin 64 de caractere, selectaţi în caseta **Pre-shared Key Format** opţiunea **Hex (64 characters)**.

- Pentru a filtra accesul în reţea a calculatoarelor, se poate înregistra adresa MAC a plăci de reţea din fiecare calculator în dispozitivul Access Point, utilizând **MAC Filtering** din meniul principal. În fereastra **MAC Address Filtering** din figura 2.2.6 se pot adăuga adresele MAC a calculatoarelor respective.

  Pentru a afla adresa MAC a plăcii de reţea dintr-un calculator activaţi butonul **Start** apoi selectaţi **Run**. În caseta care se deschide ecrieţi **cmd** apoi activaţi butonul **OK**. În fereastra care se deschide scrieţi **ipconfig/all** iar la opţiunea **Physical Address** din **Ethernet adapter Wireless Network Connection** va apărea [illegible]

MAC Address Filtering

For security reason, the Access Point features MAC Address Filtering that only allows authorized MAC Addresses associating to the Access Point.

- MAC Address Filtering Table

MAC Addres	Comment	Select
00:16:44:a6:fa:ce	Laptop Cornel	☐

Delete Selected | Delete All | Reset

☑ Enable Wireless Access Control

New | MAC Address: 0013CE177CB9 | Comment: Laptop Katy | Add | Clear

Figura 2.2.6

- Bifaţi **Enable Wireless Access Control**

  În caseta **MAC Address** introduceţi adresa MAC a plăcii de reţea in forma care este descrisă în figura 2.2.6

  În caseta **Comment** introduceţi comentarii referitoare la calculatorul respectiv

  Apăsaţi butonul **Add** şi adresa va apare în casete **MAC Address Filtering Table**

- După efectuarea setărilor, acestea pot fi salvate într-un document de pe hard disk-ul calculatorului prin activarea opţiunii **Configuration Tool** din meniu.

- În fereastra din figura 2.2.7 activaţi butonul **Save...** şi salvaţi fisierul **config.bin** într-un document de pe hard disk-ul calculatorului.

Configuration Tool

Use the "Backup" tool to save the Access Point's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Access Point. Alternatively, you can use the "Restore to Factory Default" tool to force the Access Point to perform System Reset and restore the original factory settings.

Backup Settings : Save...

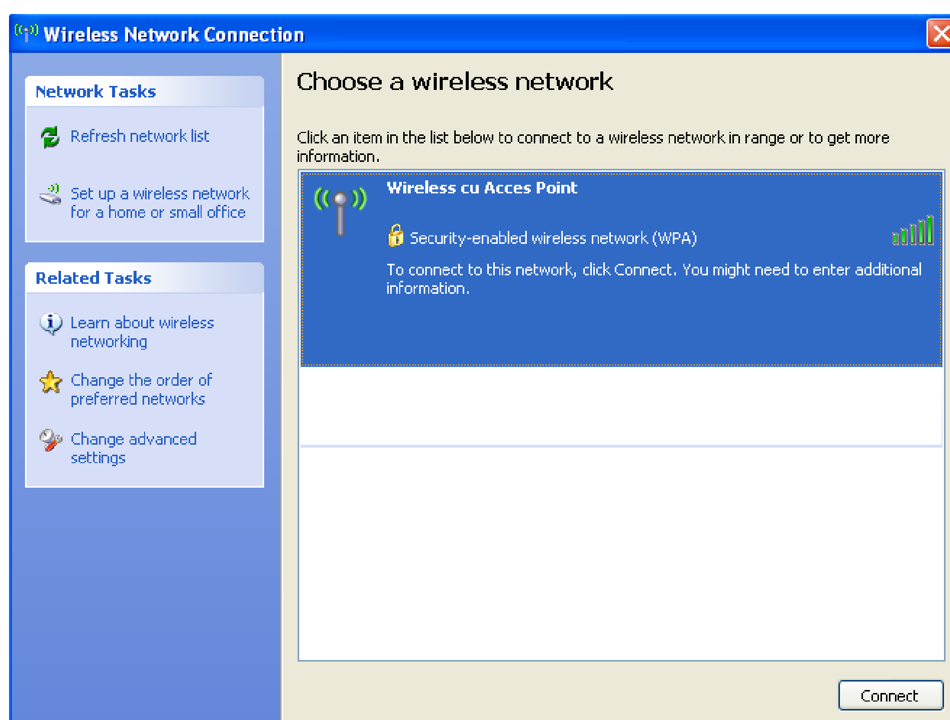
Restore Settings : Browse... Upload

Restore to Factory Default : Reset

Figura 2.2.7

B. Conectarea calculatoarele în reţea , se face parcurgând următorii paşi:

- Activaţi placa wireless de pe laptop
- Faceţi dublu clic cu butonul stâng al mouse-ului pe iconul conexiunii din tray icon, se deschide fereastra din figura 2.2.8



- Verificaţi da... ...pe **Access Point** astfel:

Selectaţi **Chan**... ...zentată în figura 2.2.8)→ **Wirele**... ...nidă ferestra din figura 2.2.9.

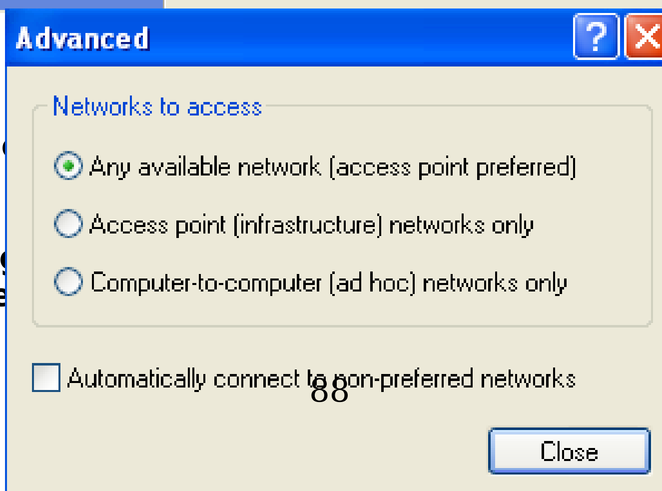
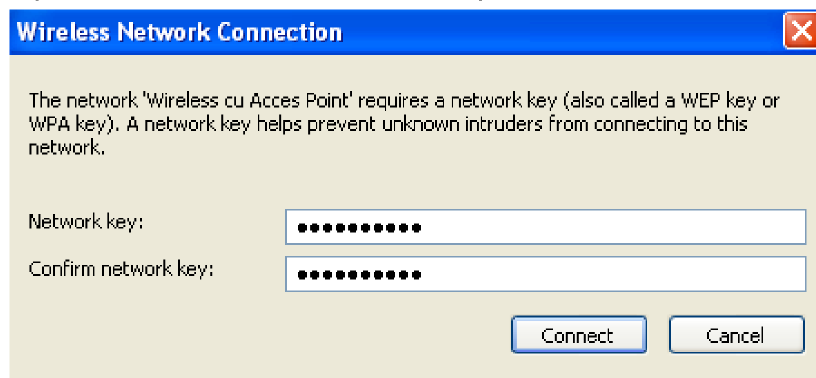


Figura 2.2.9

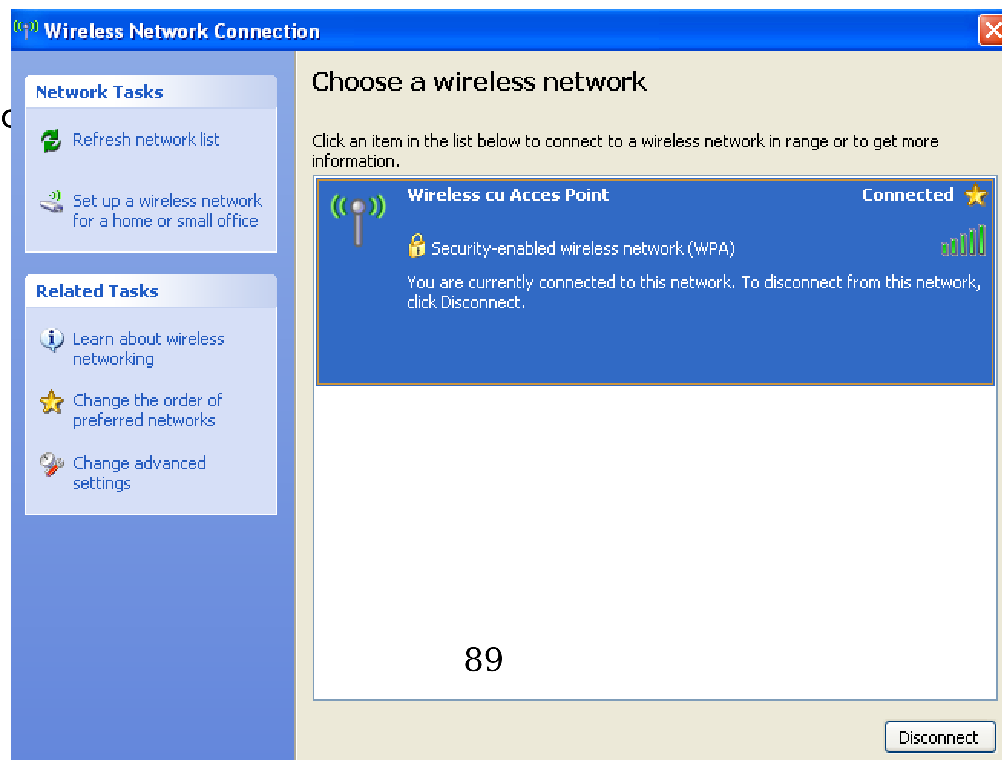
- Bifaţi opţiunea **Any available network (access point preferred)**

- Deschideţi din nou fereastra **Wireless Newtwork Connection**

- Activaţi butonul **Connect** iar în ferestra care se deschide (figura 2.2.10) introduceţi parola reţelei care aţi introdus-o în meniul **Security** al dispozitivului **Access Point**, apoi activaţi butonul **Connect**



- Dac … .2.11



C. Conectarea dispozitivului Access Point la o reţea internet.

Eliberaţi portul RJ 45 al AP, apoi conectaţi Ap la reţeaua internet

Fiecare calculator din reţeaua wireless configurată, alocă un **IP** automat, proprii plăci de reţea wireless.



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea, demonstraţia, experimentul.
- Se aplică lecţii de laborator cu tema: **“ Crearea unei reţele wireless cu access point”**
- Clasa poate fi organizată pe grupe de câte 2 elevi

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic
- Fişe de laborator
- Laptop-uri şi PC-uri prevăzute cu plăci de reţea wireless

- Dispozitive Access Point



Ca probe de evaluare se pot folosi:

- Probe practice

Tema 3. Metode de depanare pentru echipamentele de calcul portabile

Fişa suport 3.1 Descrierea procesului de depanare a unui laptop

Ce?



Procesul de depanare constă în ***analizarea*** problemelor hardware şi software în cazul unui defect, ***determinarea cauzelor*** care au dus la apariţia defectului pentru a putea localiza şi ***remedia*** defectul.



În cadrul procesului de depanare trebuie să parcurgeţi următoarele etape:

- **Colectaţi informaţii de la client** – în această etapă adresaţi clientului o serie de întrebări cu scopul de a determina cauzele care au dus la apariţia defectului:
  - Laptop-ul este conectat la priză sau foloseşte acumulatorul?
  - Laptop-ul se iniţializează şi afişează sistemul de operare?
  - Care este starea de încărcare a acumulatorului?
  - A fost instalat un soft recent?
  - Este instalat şi actualizat un program antivirus?
  - Au fost făcute setări în BIOS şi/sau la sistemul de operare?
- **Verificaţi problemele evidente**:
  - Verificaţi dacă laptop-ul este alimentat cu tensiune
  - Verificaţi starea de încărcare a acumulatorului
  - Verificaţi conexiunile la dispozitivele periferice
  - Verificaţi starea leduri-lor de semnalizare
  - Verificaţi tastele (în mod special tastele de funcţii)
- **Încercaţi soluţiile rapide de depanare**:
  - Restartaţi laptop-ul
  - La pornirea laptop-ului ţineţi apăsată tasta **F8** iar din meniul care se afişează selectaţi **Last Known Good Configuration** (***Ultima configuraţie funcţională***)

- Verificaţi setările din BIOS
- Deconectaţi dispozitivele periferice

➢ **Colectaţi informaţii de la laptop**:

- Urmăriţi secvenţa de mesaje audio scurte (dacă există)
- Citiţi eventualele mesaje de eroare la rularea programului **POST** (Power On Self Test)
- Citiţi eventualele mesaje de eroare la iniţializarea sistemului de operare
- Verificaţi în **Device Manager** (***Manager Dispozitive***) lista cu hardware-ul instalat pe laptop

Click cu butonul drept al mouse-ului pe **My Computer → Properties → Hardware → Device Manager**

➢ **Evaluaţi problema şi implementaţi soluţia**:

- Consultaţi manualul de utilizare a laptop-ului
- Căutaţi informaţii pe internet
- Consultaţi site-ul oficial al producătorului
- Utilizaţi **Help and Support** (***Ajutor şi asistenţă***)



DEFECTE FRECVENTE ŞI METODE DE SOLUŢIONARE A ACESTORA

1. LAPTOP-UL NU PORNEŞTE

1.1. SOLUŢIONARE RAPIDĂ

1.1.1. În primul rând verificaţi dacă laptop-ul nu este blocat în **stand-by**. Apăsaţi scurt butonul de pornire. Dacă tot nu porneşte ţineţi apăsat butonul de pornire câteva secunde pentru a oprii laptop-ul dacă este blocat, apoi apăsaţi din nou butonul de pornire.

1.1.2. Dacă laptop-ul este conectat prin intermediul unui adaptor la o priză de curent alternativ, verificaţi: tensiunea la priza de alimentare, conexiunile dintre adaptor şi cablurile acestuia, tensiunea de ieşire a adaptorului. În cazul în care indicatorul luminos de alimentare din partea frontală a laptop-ului clipeşte rapid, adaptorul trebuie înlocuit.

1.1.3. Dacă valorile tensiunilor măsurate la punctul **1.1.1** sunt corecte şi laptop-ul nu porneşte, scoateţi acumulatorul laptop-ului şi încercaţi din nou numai cu alimentarea de la adaptor (înainte de

a scoate acumulatorul, scoateţi mufa de alimentare de la adaptorul de curent alternativ)

1.1.4. Dacă laptop-ul porneşte atunci acumulatorul trebuie înlocuit. Înainte de înlocuirea acumulatorului, introduceţi acumulatorul în laptop, scoateţi cablul de alimentare de la adaptor şi verificaţi indicatorul luminos din partea frontală a laptop-ului. Dacă acesta clipeşte rapid însemnă că acumulatorul este descărcat. Conectaţi laptop-ul prin intermediul adaptorului la o priză şi lăsaţi acumulatorul să se încarce.

1.1.5. Deconectaţi dispozitivele periferice ale laptop-ului, resetaţi laptop-ul inserând vârful unei agrafe în butonul **Reset** (dacă laptop-ul este prevăzut cu buton Reset acesta este situat pe panoul inferior – sub laptop). După ce aţi resetat apăsaţi din nou butonul de pornire.

1.1.6. Dacă adaptorul şi acumulatorul funcţionează în parametrii normali şi laptop-ul nu porneşte, atunci urmaţi paşii soluţionării amănunţite.

1.2. SOLUŢIONAREA AMĂNUNŢITĂ

1.2.1. Verificaţi căile de ventilaţie. Dacă este cazul demontaţi laptop-ul şi curăţaţi căile de ventilaţie şi cooler-ul laptop-ului.

1.2.2. Deconectaţi laptop-ul de la sursele de energie pentru câteva minute. Conectaţi laptop-ul, apăsaţi butonul de pornire, iar dacă în momentul repornirii se aud zgomote ciudate din zona **hard disck-ului**, atunci acesta trebuie verificat sau înlocuit.

1.2.3. Verificaţi contactul butonului de pornire

1.2.4. Verificaţi modulele de **memorie RAM**. Dacă sunt 2 module, scoateţi pe rând câte un modul şi verificaţi dacă laptop-ul porneşte cu modulul rămas. Dacă porneşte cu un singur modul înseamnă că modulul scos este defect.

1.2.5. Verificaţi **cooler-ul** procesorului. Dacă este defect placa de bază nu permite pornirea laptop-ului.

1.2.6. Verificaţi **procesorul**, dacă este cazul înlocuiţi procesorul cu alt procesor de la acelaşi producător (dacă este permisă înlocuirea).

1.2.7. Dacă laptop-ul este prevăzut cu placă video dedicată, verificaţi **placa video**. Scoateţi placa video şi verificaţi dacă laptop-ul porneşte.

2. ECRANUL LAPTOP-ULUI NU LUMINEAZĂ

2.1. SOLUŢIONARE RAPIDĂ

2.1.1. În primul rând verificaţi dacă laptop-ul nu este în **stand-by**. Procedaţi ca la punctul **1.1.1**

2.1.2. Verificaţi dacă laptop-ul nu **este comutat pe monitor extern**. Apăsaţi o tastă sau apăsaţi de câteva ori tasta **Fn** şi tasta **funcţională** care se foloseşte pentru comutare pe monitor extern.

2.1.3. Dacă la apăsarea tastei **Caps Lock** (tasta cu simbolul ⇩), indicatorul luminos corespunzător tastei se aprinde, **conectaţi un monitor extern** la laptop. Apăsaţi tasta **Fn** şi tasta **funcţională** utilizată pentru comutarea pe monitor extern şi observaţi dacă pe monitor apare imagine.

2.1.4. Dacă pe monitorul extern este imagine, atunci defectul este la display-ul laptop-ului situaţie în care urmaţi paşii **2.2.2 – 2.2.7** de la soluţionarea amănunţită

2.1.5. Dacă pe monitorul extern nu este imagine, urmaţi paşii **2.2.8 – 2.2.9** de la soluţionarea amănunţită.

2.2. SOLUŢIONAREA AMĂNUNŢITĂ

2.2.1. Demontaţi capacul laptop-ului şi verificaţi conexiunile dintre display şi placa de bază, eventual cablurile panglică care merg spre display.

2.2.2. Demontaţi display-ul şi verificaţi conexiunile la **invertor** (care se află în partea de jos a disply-ului între balamale). Invertorul este un dispozitiv care asigură tensiunea de alimentare a lămpii de fundal (**CCFL, *cold cathode fluorescent lamp*-lampa fluorescenta cu catod rece**).

2.2.3. Verificaţi siguranţa fuzibilă SMD a invertorului

2.2.4. Verificaţi tensiunea de alimentare a invertorului.

2.2.5. Verificaţi conexiunile dintre invertor şi lampa de fundal CCFL.

2.2.6. Verificaţi funcţionarea lămpii de fundal care se află în partea superioară a display-ului, pe toată lungimea acestuia. Observaţi dacă lampa are defecte, eventual schimbaţi lampa.

2.2.7. Dacă display-ul este de tip **x-blank (are iluminarea cu led-uri)**, atunci depanarea lui este mai dificilă .

2.2.8. Dacă pe monitorul extern nu este imagine, verificaţi, în primul rând, placa video a laptop-ului.

2.2.9. Dacă placa video este integrată pe placa de bază trebuie verificată placa de bază.

2.2.10. Dacă nici una din metodele prezentate nu a dus la soluţionarea defectului, trebuie înlocuit display-ul.

3. LAPTOP-UL PORNEŞTE DAR SISTEMUL DE OPERARE NU SE INIŢIALIZEAZĂ

3.1. SOLUŢIONARE RAPIDĂ

3.1.1. Porniţi calculatorul şi apăsaţi tasta **F8** de mai multe ori consecutiv

3.1.2. În meniul **Windows Advanced Options** care se deschide, utilizaţi comanda **Last Known Good Configuration** (***Ultima configuraţie funcţională***).

3.1.3. Dacă sistemul de operare nu se iniţializează porniţi din nou calculatorul şi apăsaţi iarăşi tasta **F8** iar din meniul care se deschide selectaţi **Safe Mode**

3.1.4. Dacă sistemul de operare se iniţializează (în Safe Mode) dezinstalaţi ultima aplicaţie adăugată utilizând **Add/Remove program** din **Control Panel**

3.1.5. Verificaţi aplicaţia **Device Manager** în vederea depistării conflictelor între dispozitive

3.1.6. Faceţi o scanare de viruşi şi spyware.

3.1.7. Reveniţi la setările anterioare ale sistemului utilizând **System Restore**

Start→ Programs→ Accessories→ System Tools→System Restore

3.1.8. Dacă nu aţi reuşit să soluţionaţi problema din **Safe Mode** porniţi laptop-ul şi intraţi în **BIOS** (***Basic Input Output System***), (la pornire apăsaţi tasta **F2** sau tasta **Del**)

3.1.9. Utilizaţi funcţia **Load BIOS Defaults** pentru a reveni la valorile iniţiale ale BIOS-ului

3.1.10. Utilizaţi funcţia **Auto detect** pentru a detecta automat hard disk-ul

NU FACEŢI SETĂRI ÎN BIOS DACĂ NU CUNOAŞTEŢI BINE FUNCŢIILE ACESTUIA.

3.1.11. Dacă nici una din metodele prezentate nu a dus la soluţionarea defectului, urmaţi paşii de la soluţionarea amănunţită.

3.2. SOLUŢIONARE AMĂNUNŢITĂ

3.2.1. Stabiliţi dacă natura cauzei defectului are la bază o componentă hardware. În acest scop verificaţi:

3.2.1.1. Modulele de memorie RAM – acest defect se manifestă deseori prin apariţia unui ecran albastru şi a unui mesaj de eroare. Pentru a remedia acest defect opriţi calculatorul, scoateţi cablul de alimentare şi acumulatorul, apoi scoateţi modulele de memorie curăţaţi contactele sau eventual încercaţi să le înlocuiţi.

3.2.1.2. Hard disk-ul – pe HDD există fişiere de sistem deteriorate, pot fi defecţiuni fizice sau nu porneşte. Pentru a remedia defectul în primul rând verificaţi alimentarea hard disk-ului şi cablul de date al acestuia. Încercaţi scanarea şi recuperarea sectoarelor defecte cu un program specializat în aceste operaţii (HDD Regenerator, SpinRite, TestDisk). Dacă defectul nu poate fi remediat, partiţia pe care este instalat sistemul trebuie formatată iar sistemul trebuie instalat din nou. Consideraţi formatarea ca o ultimă soluţie în rezolvarea problemei.

3.2.1.3. Dispozitive şi drivere instalate recent. Această situaţie apare atunci când driver-ul care s-a utilizat pentru instalarea unui dispozitiv nu este compatibil cu sistemul de operare utilizat. Pentru remedierea problemei, dezinstalaţi driver-ul, înlăturaţi dispozitivul şi reporniţi laptop-ul.

3.2.1.4. Placa de bază – în cele mai multe cazuri, un condensator defect de pe placa de bază, poate provoca acet tip de defect.

3.2.2. Stabiliţi dacă defectul este de natură software. Cauzele cele mai frecvente care duc la acest defect sunt:

3.2.2.1. Coruperea fişierelor NTLDR şi/sau **ntdetect.com** – în această situaţie, după pornirea calculatorului apare mesajul

NTLDR is missing Pentru rezolvarea acestei probleme procedaţi astfel:

- Introduceţi în CD-ROM, CD-ul cu kit-ul de instalare a WIN XP
- Porniţi laptop-ul
- Când apare mesajul **Welcome to Setup** apăsaţi tasta **R**, pentru a porni **Consola de Recuperare**
- Apăsaţi tasta **1**, apoi apăsaţi tasta **ENTER**
- Introduceţi parola de Administrator
- După ce apare promptul Consolei de recuperare scrieţi comenzile:
    - **copy e:\i386\ntldr c:\ <press enter>**
    - **copy e:\i386\ntdetect.com c:\ <press enter>**

    (aici unitatea **e:** este considerată unitatea optică)

    Prin aceste comenzi se copiază fişierele ntldr şi ntdetect.com de pe CD (în cazul nostru unitatea e:) pe partiţia c:
- După ce fişierele au fost copiate cu succes, scoateţi CD-ul şi restartaţi laptop-ul.

3.2.2.2. Coruperea fişierului boot.ini – în acestă situaţie după pornirea laptop-ului poate apare mesajul:

invalid boot.ini file ***Booting from C:/Windows***

Pentru rezolvarea problemei porniţi **Consola de Recuperare**, ca la punctul **3.2.2.1** apoi scrieţi comenzile:

c: <press enter>
cd\ <press enter>
attrib -r -a -s -h boot.ini <press enter>
edit boot.ini <press enter>

Restartaţi laptop-ul.



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- sala de clasă
- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea.
- Clasa poate fi organizată frontal sau pe grupe

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic
- Fişe de lucru pentru elevi



Ca probe de evaluare se pot folosi:

- Probe orale
- Teste scrise

Tema 4. Depanare unor echipamente de calcul portabile

Fişa suport 4.1 Înlocuirea acumulatorului şi hard disk-ului unui laptop

A. ÎNLOCUIREA ACUMULATORULUI



Scoaterea acumulatorului (**figura 4.1.1**)

- Întoarceţi laptop-ul cu compartimentul acumulatorului în sus
- Acţionaţi dispozitivul de blocare (**1**) spre dreapta
- Acţionaţi dispozitivul dispozitivul (**2**) de prindere al acumulatorului spre dreapta
- Scoateţi acumulatorul (**3**) din laptop

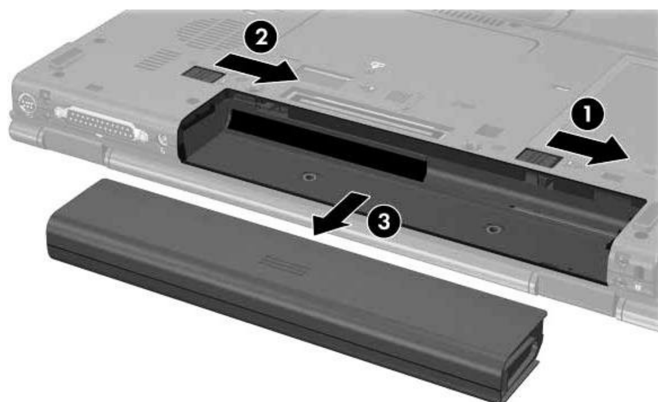


Figura 4.1.1 Scoaterea acumulatorului din laptop



Introducerea acumulatorului (**figura 4.1.2**)

- Întoarceţi laptop-ul cu compartimentul acumulatorului în sus
- Introduceţi acumulatorul laptop-ului (**1**) în compartimentul său până la fixare
- Dispozitivul (**2**) fixează acumulatorul în compartiment

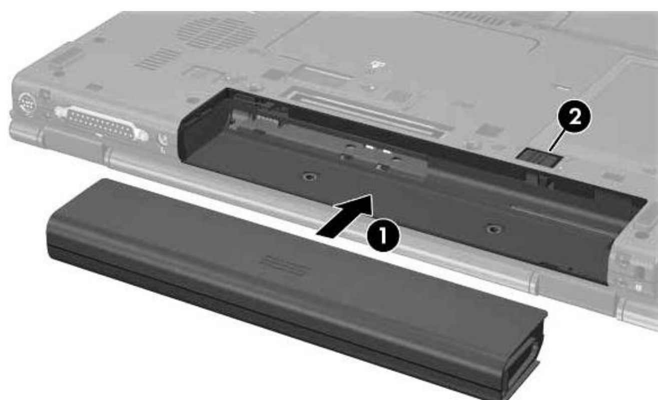


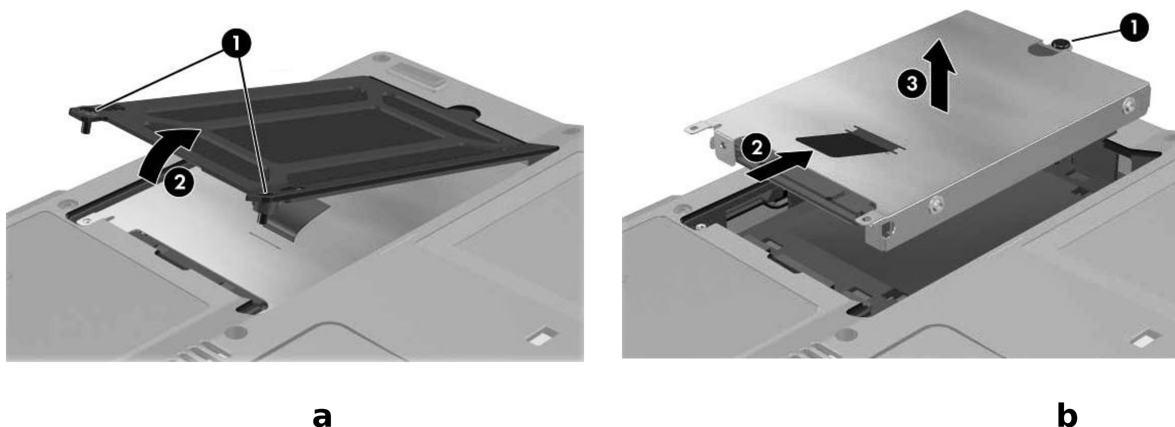
Figura 4.1.2 Introducerea acumulatorului în laptop

B. ÎNLOCUIREA HARD DISK-ULUI



Scoaterea hard disk-ului (**figura 4.1.3**)

- Închideţi laptop-ul şi scoateţi cablul de alimentare de la reţeaua electrică
- Scoateţi acumulatorul laptop-ului
- Întoarceţi laptop-ul cu ecranul în jos
- Scoateţi cele două şuruburi (**1**) – **fig. 4.1.3 a**
- Ridicaţi capacul compartimentului hard disk-ului (**2**) – **fig. 4.1.3 a** şi îndepărtaţil
- Desfaceţi şurubul hard disk-ului (**1**) – **fig. 4.1.3 b**
- Deconectaţi hard disk-ul prin tragerea **spre dreapta** a foliei (**2**) – **fig. 4.1.3 b**
- Scoateţi hard disk-ul din laptop (**3**) – **fig. 4.1.3 b**



a **b**

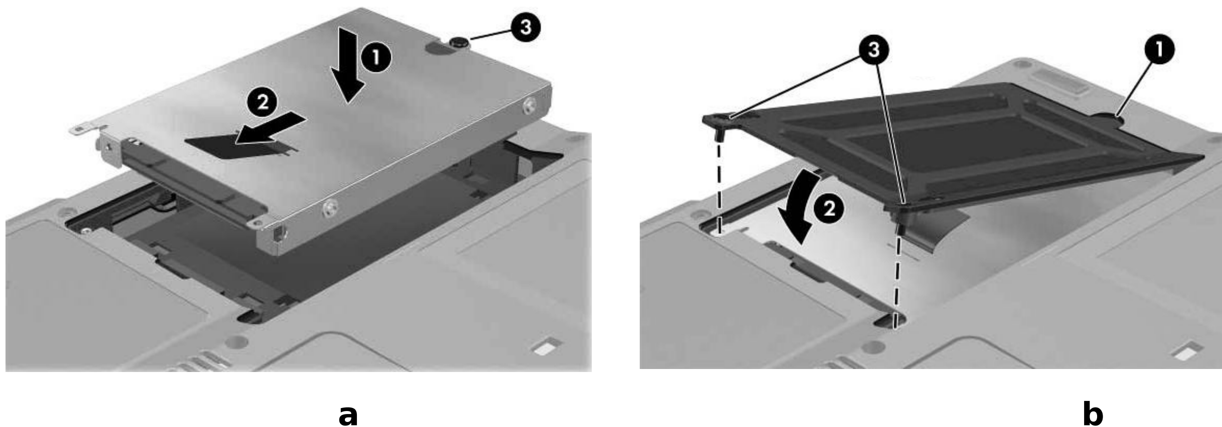
Figura 4.1.3 Scoaterea unui hard disk din laptop



Introducerea hard disk-ului (**figura 4.1.4**)

- Introduceţi hard disk-ul în compartimentul său aflat în partea din spate a laptop-ului (**1**) – **fig. 4.1.4 a**
- Conectaţi hard disk-ul prin tragerea spre **stânga** a foliei (**2**) – **fig. 4.1.4 a**

- Montaţi şurubul hard disk-ului (**3**) – **fig. 4.1.4 a**
- Montaţi capacul compartimentului hard disk-ului (**1**) – **fig. 4.1.4 b**
- Închideţi capacul compartimentului hard disk-ului (**2**) – **fig. 4.1.4 b**
- Montaţi şuruburile capacului (**3**) – **fig. 4.1.4 b**



a **b**

Figura 4.1.4 Introducerea unui hard disk în laptop



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

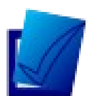
- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea, demonstraţia, experimentul.
- Se pot aplica lecţii de laborator cu tema: **„Demontarea/montarea subansablelor unui laptop"**
- Clasa poate fi organizată pe grupe de 3 – 4 elevi.

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic
- Fişe de laborator
- Laptop-uri care pot fi demontate
- Acumulatori şi HDD-uri laptop

**Ca probe de evaluare** se pot folosi:

- Probe practice

Fişa suport 4.2 Înlocuirea tastaturii unui laptop

În funcţie de modelul laptop-ului, în majoritatea cazurilor, demontarea tastaturii se face în două moduri

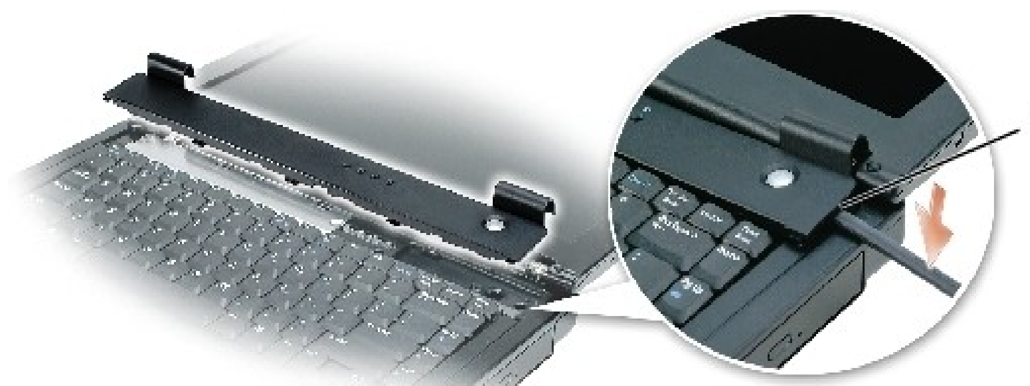


Demontarea tastaturii la care şuruburile de prindere sunt situate în partea frontală a laptop-ului, se face parcurgând următorii paşi:

- Închideţi laptop-ul şi scoateţi cablul de alimentare de la reţeaua electrică
- Scoateţi acumulatorul laptop-ului
- Desfaceţi apărătorile de la balamalele display-ului (**1**) – **fig. 4.2.1 a**
- Rabataţi ecranul laptop-ului la 180°, apoi scoateţi apărătoarea care este situată deasupra tastelor **F** (**1**) – **fig. 4.2.1 b**
- Dacă tastatura este prinsă cu două şuruburi, desfaceţi aceste şuruburi, apoi rabataţi tastatura la 45° dinspre monitor – **fig. 4.2.2 a**
- Dacă tastatura nu este prinsă cu şuruburi, atunci rabataţi tastatura la 45° dinspre monitor (**1**) – **fig. 4.2.2 b**
- Scoateţi cablul panglică al tastaturii din conectorul fixat pe placa de bază (**2**) – **fig. 4.2.2 b**

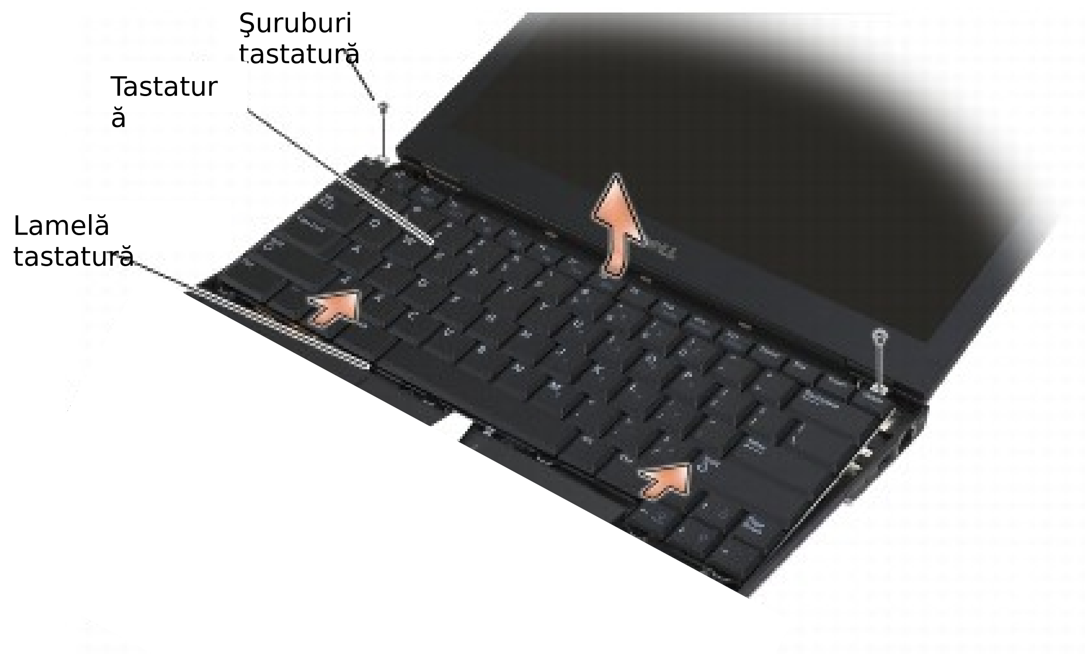


a



b

Figura 4.2.1 Demontarea tastaturii unui laptop



a



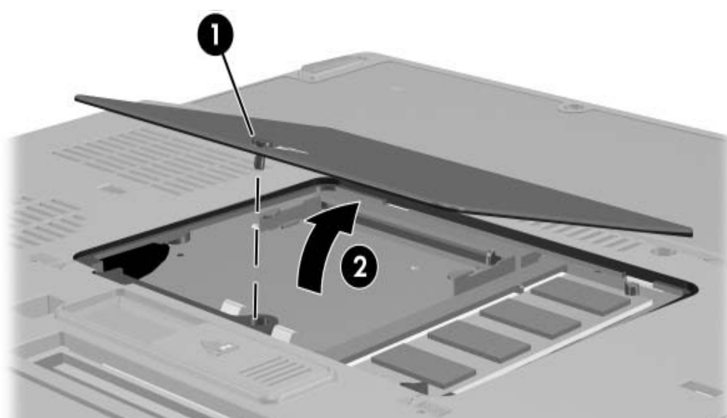
b

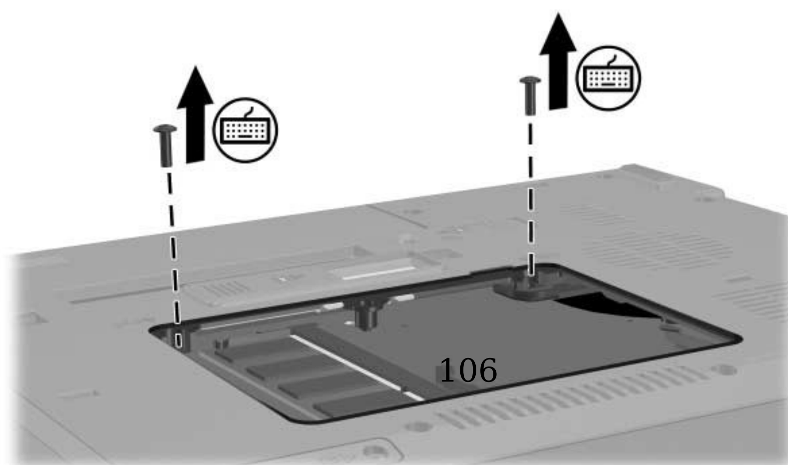
Figura 4.2.2 Demontarea tastaturii unui laptop



Demontarea tastaturii la care şuruburile de prindere sunt situate în partea din spate a laptop-ului, se face parcurgând următorii paşi:

- Închideţi laptop-ul
- Deconectaţi dispozitivele externe conectate la laptop
- Scoateţi cablul de alimentare şi acumulatorul
- Întoarceţi laptop-ul cu ecranul în jos
- Desfaceţi şurubul capacului (**1**) – **fig. 4.2.3 a**
- Ridicaţi capacul (**2**) – **fig. 4.2.3 a**
- Scoateţi cele două şuruburi ale tastaturii – **fig. 4.2.3 b**
- Întroarceţi laptop-ul invers şi deschideţi-l
- Deblocaţi suporţii de prindere a tastaturii (**1**) – **fig. 4.2.4 a**
- Ridicaţi partea superioară a tastaturii cu grijă – **fig. 4.2.4 b**





b

Figura 4.2.3 Demontarea tastaturii unui laptop



a



b

Figura 4.2.4 Demontarea tastaturii unui laptop

Pentru montarea tastaturii se urmează paşii explicaţi la demontarea tastaturii, dar în ordine inversă



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea, demonstraţia, experimentul.
- Se pot aplica lecţii de laborator cu tema: **„Demontarea/montarea subansablelor unui laptop”**
- Clasa poate fi organizată pe grupe de 3 – 4 elevi.

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic
- Fişe de laborator
- Laptop-uri care pot fi demontate
- Tastaturi laptop



Ca probe de evaluare se pot folosi:

- Probe practice

Fişa suport 4.3 Înlocuirea sloturilor de memorie ale unui laptop



Pentru înlocuirea **modulului de memorie RAM din slotul de extensie** parcurgeţi următorii paşi:

- Închideţi laptop-ul şi scoateţi cablul de alimentare cu tensiune
- Întroarceţi laptop-ul cu ecranul în jos
- Scoateţi acumulatorul
- Desfaceţi şuruburile capacului (**1**) – **fig. 4.3.1 a**
- Ridicaţi şi înlăturaţi capacul (**2**) – **fig. 4.3.1 a**
- Depărtaţi suporţii de prindere de pe părţile laterale ale modulului, pentru a elibera modulul (**1**) – **fig. 4.3.1 b**
- Prindeţi modulul de părţile laterale şi trăgeţi-l încet din slot (**2**) – **fig. 4.3.1 b**
- Înainte de introduce în slot modulul nou, aliniaţi cheia modulului cu tab-ul slotului (**1**) – **fig. 4.3.1 c**
- Introduceţi modulul în slot sub un unghi de 45° şi apăsaţi până la fixare (**2**) – **fig. 4.3.1 c**
- Apăsaţi modulul până când suporţii se fixează (**fig. 4.3.1 d**)
- Montaţi capacul modulului (**1**) – **fig. 4.3.1 e**
- Prindeţi şurubul capacului (**2**) – **fig. 4.3.1 e**
- Montaţi acumulatorul
- Reconectaţi cablul de alimentare şi dispozitivele externe
- Porniţi la ţionează corect
- Verificaţ

Click cu butonul c **mputer→ Properties→ se deschide fer**

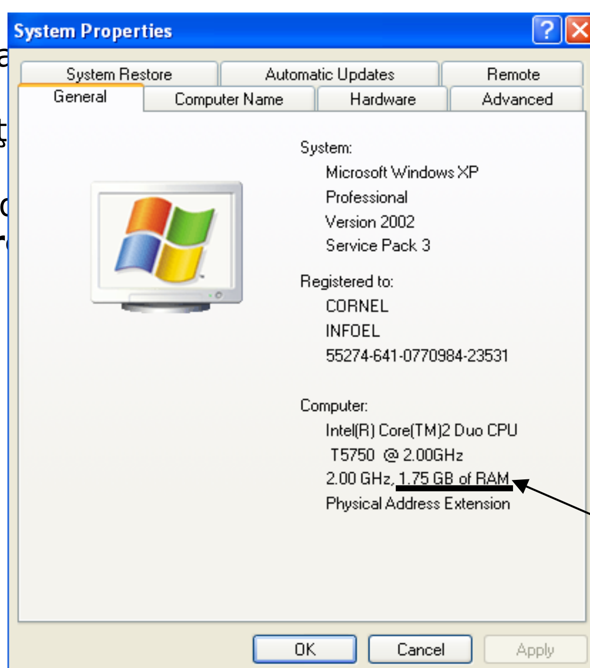
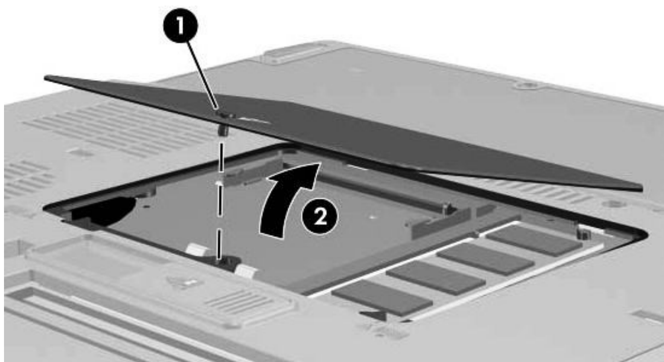
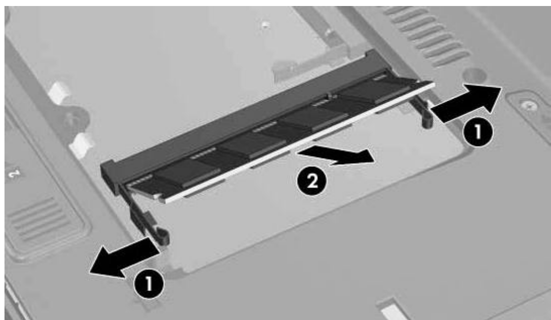


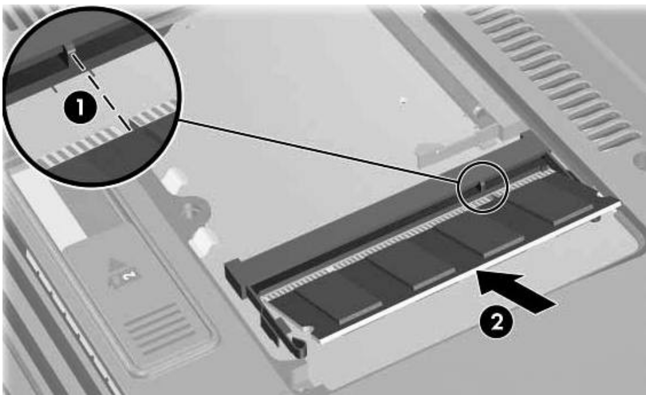
Figura 4.3.1



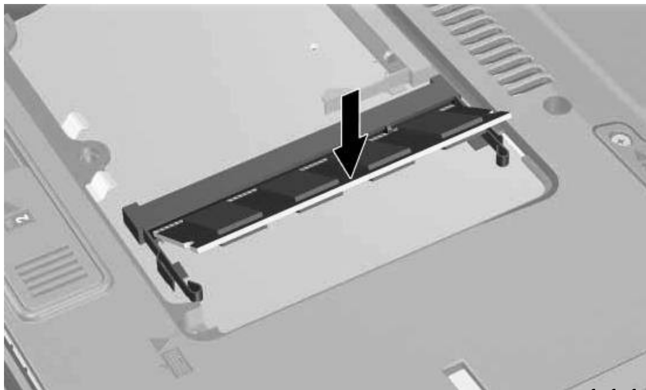
a



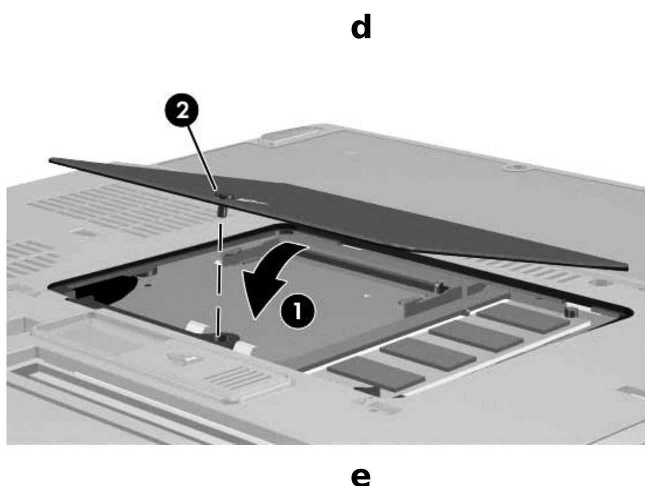
b



c



d



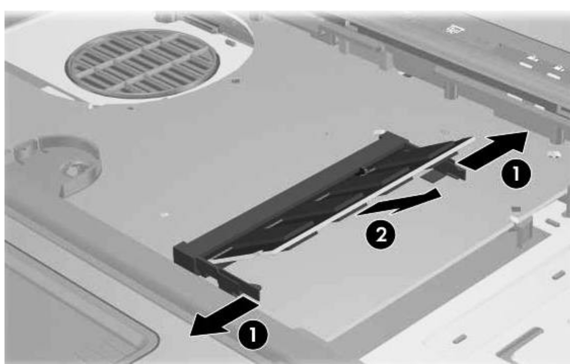
e

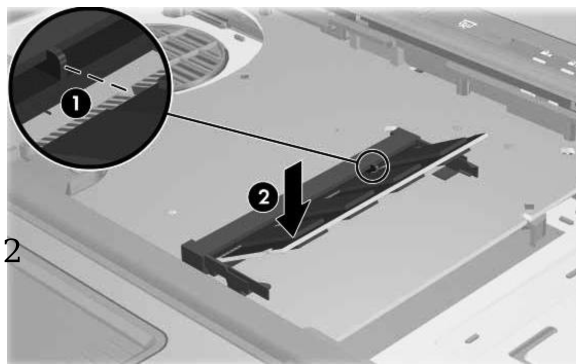
Figura 4.3.1 Înlocuirea modulului de memorie RAM din slotul de extensie



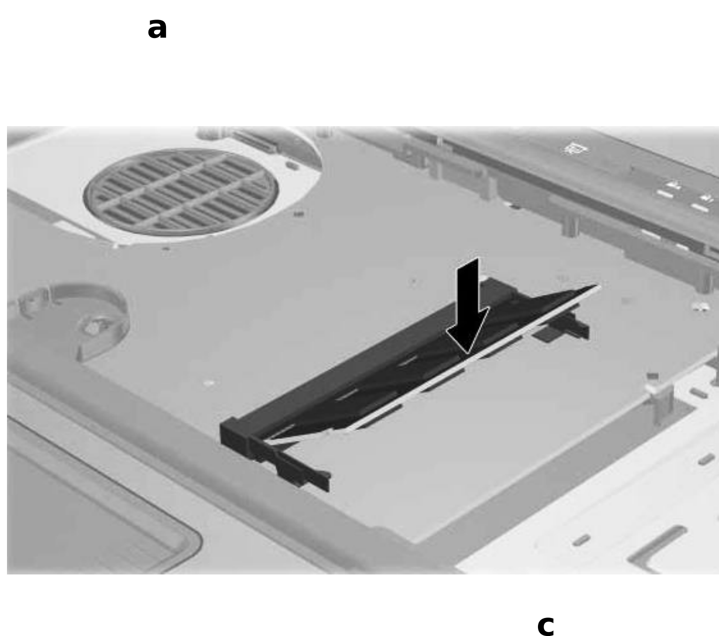
Pentru înlocuirea **modulului de memorie RAM din slotul primar** parcurgeţi următorii paşi:

- Demontaţi tastatura (vezi **Fişa suport 4.2**)
- Depărtaţi suporţii de prindere de pe părţile laterale ale modulului (**1**) – **fig. 4.3.2 a**
- Prindeţi modulul de părţile laterale şi trăgeţi-l uşor din slot (**2**) – **fig. 4.3.2 b**
- Înainte de a introduce modulul nou în slot aliniaţi cheia modulului cu tab-ul slot-ului (**1**) **fig. 4.3.2 b**
- Introduceţi modulul în slot sub un unghi de 45° şi apăsaţi până la fixare (**2**) – **fig.4.3.2 b**
- Apăsaţi modulul până când suporţii se fixează (**fig. 4.3.2 c**)
- Montaţi tastatura (vezi **Fişa suport 4.2**)
- Montaţi acumulatorul
- Reconectaţi cablul de alimentare şi dispozitivele externe
- Verificaţi funcţionarea laptop-ului.





a **b**



c

Figura 4.3.2 Înlocuirea modulului de memorie RAM din slotul primar



Sugestii metodologice

Unde?

Conţinutul poate fi predat în :

- laboratorul de informatică

Cum?

- Se utilizează ca metode de predare: conversaţia dirijată, explicaţia, problematizarea, demonstraţia, experimentul.
- Se pot aplica lecţii de laborator cu tema: **„Demontarea/montarea subansablelor unui laptop”**

- Clasa poate fi organizată pe grupe de 3 – 4 elevi.

Cu ce?

- Videoproiector multimedia şi flipchart
- Fişe Power Point pentru prezentarea materialului didactic
- Fişe de laborator
- Laptop-uri care pot fi demontate
- Module memorie RAM laptop



Ca probe de evaluare se pot folosi:

- Probe practice

IV. Bibliografie

[1]Bruce Hopkins, Ranjith Antony , “**Bluetooth for Java**”, Apress , 2003

[2]Bluetooth Special Interest Group (SIG), “**BLUETOOTH SPECIFICATION Version 2.0 + EDR [vol 0]**: Specification of the Bluetooth System”,2004

[3]Bluetooth Special Interest Group (SIG), “**Volume 4_SPEC**”, 2006

[4]Roger Riggs, Antero Taivalsaari, Jim Van Peursem, “**Programming Wireless Devices with the Java 2 Platform, MicroEdition, Second Edition**”, Addison Wesley, 2003

[5]Jonathan Knudsen ,“**Wireless Java Developing with J2ME**, Second Edition”, Apess, 2003

[6]Heikki Ailisto, “**Physical browsing with NFC technology**”

[7]GSMA, “**Mobile NFC Services**”